FACULTAD DE INGENIERÍA Y COMPUTACIÓN

PROGRAMA PROFESIONAL DE INGENIERÍA DE TELECOMUNICACIONES

TESIS DE GRADO

Sistema de Seguridad en Capa Física empleando Descomposición Algebraica del Canal para Sistemas de Comunicaciones Inalámbricas OFDM

Autor: Francisco Javier Guerra Manchego
Bachiller en Ingeniería de Telecomunicaciones

Orientador: Alex Cartagena Gordillo
Dr. en Radiocomunicaciones

Tesis profesional presentada al Programa Profesional de Ingeniería de Telecomunicaciones como parte de los requisitos para obtener el Título Profesional de Ingeniero de Telecomunicaciones.

Arequipa, mayo de 2017

TESIS DE GRADO

SISTEMA DE SEGURIDAD EN CAPA FÍSICA EMPLEANDO DESCOMPOSICIÓN ALGEBRAICA DEL CANAL PARA SISTEMAS DE COMUNICACIONES INALÁMBRICAS OFDM

Autor: Francisco Javier Guerra Manchego

Orientador: Dr. Alex Cartagena Gordillo

Tesis de grado presentada en el cumplimiento de los requisitos para obtener el título profesional de Ingeniero de Telecomunicaciones.

Firma del Jurado Evaluador:

		Firma
Presidente:	Dr./Mag./Ing. Nombre y Apellidos	_____
Vocal:	Dr./Mag./Ing. Nombre y Apellidos	_____
Secretario:	Dr./Mag./Ing. Nombre y Apellidos	_____
Suplente:	Dr./Mag./Ing. Nombre y Apellidos	_____

Calificación:

Arequipa, ____ de _____ de 2017

"El científico no estudia la naturaleza porque es útil, la estudia porque se deleita en ella, y se deleita en ella porque es hermosa"

Henri Poincaré, 1854-1912

Índice general

Abstract **5**

Resumen **6**

1. Introducción **7**
1.1. Motivación y Contexto 8
1.2. Planteamiento del problema 8
1.3. Objetivos 9
1.3.1. Objetivo general 9
1.3.2. Objetivos específicos 9
1.4. Organización del trabajo 9

2. Marco Teórico **10**
2.1. Redes Inalámbricas 10
2.1.1. Clasificación de Redes Inalámbricas basado en cobertura . . . 10
2.1.2. Arquitectura de Redes Inalámbricas 11
2.1.3. Seguridad en Redes Inalámbricas 12
2.1.4. Vulnerabilidades en Redes Inalámbricas 13
2.2. Capa física 14
2.2.1. Descripción de la capa física basado en el estándar IEEE 802.11 14
2.3. Descomposición Algebraica 17
2.3.1. Descomposición LU 17
2.3.2. Descomposición QR 18
2.3.3. Descomposición SVD 18
2.4. Canal de propagación 19
2.5. Estimación de canal 21
2.5.1. Estimación asistida por datos 22
2.5.2. Estimación no asistida por datos 22
2.5.3. Técnicas de Estimación de Canal 22
2.6. OFDM (Orthogonal Frecuency Division Multiplexing) 26
2.6.1. Transmisor OFDM 27
2.6.2. Receptor OFDM 28
2.6.3. Prefijo cíclico 30
2.6.4. Ventajas y desventajas de OFDM 31

3. Estado del Arte **32**
3.1. Enfoque basado en la codificación 32

3.2. Enfoque basado en potencia 33
3.3. Enfoque basado en el Diseño de la Señal 33
3.4. Enfoque basado en el Canal de Comunicación 35
3.5. Resumen 36

4. Propuesta de Solución **38**
4.1. Escenario de la Solución Propuesta 38
4.2. Descripción de la Solución Propuesta 39
4.2.1. Proceso de Saludo 39
4.2.2. Desarrollo de la Solución Propuesta 39

5. Simulaciones y resultados **43**
5.1. Software 43
5.2. Simulación de los Estimadores de Canal 43
5.3. Simulación del Sistema de Seguridad en Capa Física 46
5.3.1. Transmisor 46
5.3.2. Canal 47
5.3.3. Receptor 48
5.3.4. Simulación de la Capa Física basada en el Estándar IEEE 802.11a usando seguridad 49

6. Conclusiones y trabajos futuros **55**

Acknowledgements **57**

A. Anexo **58**

Bibliografía **60**

Nomenclatura **63**

Índice de figuras

2.1. Velocidad de Transmisión y Movilidad de las Tecnologías Inalámbricas. [LDRV07] 11
2.2. Arquitectura Inalámbrica Centralizada. [Dez07] 11
2.3. Arquitectura Inalámbrica Distribuida. [Dez07] 12
2.4. Pila de Protocolos del Estándar IEEE 802.11. [Esp11] 15
2.5. Encapsulado en la Capa MAC. [Esp11] 15
2.6. Encapsulado en la Capa Física. [Esp11] 16
2.7. Propagación multicamino [Pol11] 19
2.8. Diagrama de Bloques de Receptor OFDM en Banda Base. [Cor09] . 21
2.9. Modelo de Estimación no Asistida por Datos. [Pol11] 22
2.10. Estimador MMSE basado en la Solución Wiener-Hopf. [Mia06] [20] . 25
2.11. Espectro de señal OFDM como 6 subportadoras. [LDRV07] 27
2.12. Diagrama de Bloques de Generador de símbolo OFDM. [LDRV07] . 28
2.13. Diagrama de Bloques Receptor OFDM con correlacionadores [LDRV07] 29
2.14. Efecto ISI en los símbolos recibidos. [Val10] 30
2.15. Diagrama de Bloques de un Transmisor y Receptor OFDM. [Val10] . 30

3.1. Arquitectura de Seguridad en el Estándar IEEE 802.16. [Pra10] . . . 32
3.2. Técnica iJam [GK11] 34
3.3. BER obtenido con la técnica iJam [GK11] 34
3.4. Sistema de Seguridad usando Rotación de Símbolos [JST10a] 35
3.5. BER obtenido con el Sistema de Seguridad usando rotación de Símbolos [JST10a] 36

4.1. Escenario del Problema Estudiado 38
4.2. Proceso de Saludo 39
4.3. Diagrama de Bloques del Sistema de Seguridad. 40
4.4. Diagrama de Bloques del Transmisor/Receptor OFDM usando SVD. 42

5.1. Asignación de subportadoras en la especificación IEEE 802.11. . . . 44
5.2. Diagrama de Bloques para el cálculo del error usando LSE y MMSE. 44
5.3. Error de Estimación para LSE y MMSE. 45
5.4. Diagrama de Bloques de la Capa Física según el estándar IEEE 802.11a. 46
5.5. a) Símbolo OFDM. b) Símbolo OFDM con CP. c) Densidad espectral del símbolo OFDM sin CP. d) Densidad espectral del símbolo OFDM con CP. 47
5.6. Respuesta al impulso del canal modelado. 47

5.7. Función de densidad de probabilidad del canal. 48
5.8. Diagrama de Bloques del Sistema de Seguridad en Capa Física. . . . 49
5.9. Escenario de simulación donde el atacante realiza SVD de su canal. . 49
5.10. a) Símbolo sin encriptación. b) Símbolo encriptado. c) Densidad espectral de potencia del símbolo sin encriptación. d) Densidad espectral de potencia del símbolo encriptado. 50
5.11. a) Repuesta al impulso del canal del receptor legítimo. b) Respuesta al impulso del canal espía. 50
5.12. a) Ruido AWGN. b) Ruido AWGN multiplicado por W_k. c) Densidad espectral del ruido AWGN. d) Densidad espectral del ruido AWGN multiplicado W_k. 51
5.13. Función de densidad de probabilidad obtenida del producto entre el ruido AWGN y la matriz W_k. 51
5.14. a) Símbolo transmitido sin encriptación. b) Símbolo recibido desencriptado. c) Densidad espectral del símbolo transmitido sin encriptación. d) Densidad espectral del símbolo desencriptado. 52
5.15. Curva de BER vs E_b/N_o. 52
5.16. Escenario de simulación donde el atacante no realiza SVD de su canal. 53
5.17. Curva de BER del atacante con conocimiento de encriptación de datos 54

Índice de cuadros

2.1. Características de los Algoritmos de Estimación de Canal 23

5.1. Parámetros de Simulación basado en el estándar IEEE 802.11a. . . . 45

Abstract

Wireless Communications security is a great challenge that researchers have been addressing due to the open-access nature of the transmission medium. Most of the solutions are traditional cryptographic mechanisms that are frequently implemented at upper OSI-model layers. This thesis presents a security system at the Physical Layer considering a wireless communication system as the scenario with the presence of an eavesdropper. This scenario uses the IEEE 802.11a standard. The following system proposes to employ Algebraic Channel Decomposition, which is unique among the original transmitter and receiver, it also provides a security key by using U_k, Δ_k y V_k matrices, obtained through the decomposition process. The V_k matrix is the one that multiplies the OFDM (Othogonal Frecuency Division Multiplexing) symbols resulting on the encryption data function matrix, while at the receiver, we consider the U_k, Δ_k matrices, which represent the decrypting matrices. On the other hand, the eavesdropper, who owns a different propagation channel, will not be able to decrypt the transmitted information. The security level is quantified by comparing the BER (Bit Error Rate) values measured at the eavesdropper and the original receiver.

Simulations were carried out in two scenarios. The first one is when the eavesdropper doesn't know its propagation channel and tries to perform the decryption of symbols sent between the original transmitter and receiver. For this purpose 1000 OFDM symbols are transmitted each consisting of 52 data subcarriers modulated with BPSK (Binary Phase Shift Key), according to IEEE 802.11a standard. For this case, BER value measured is almost constant $10^{-0.3}$ for eavesdropper with different values of E_b/N_o, while BER for original receiver falls as E_b/N_o increase. In the second scenario the eavesdropper has knowledge of its propagation channel while performing the decryption of the symbols. As in the previous case, BER value measured is almost constant, $10^{-0.3}$ for different values of E_b/N_o.

Resumen

La seguridad en las comunicaciones inalámbricas es un gran desafío que se han planteado los investigadores en los últimos años debido a la naturaleza de libre acceso del medio de transmisión. La mayor parte de las soluciones vienen tradicionalmente dadas por mecanismos criptográficos que se implementan en las capas superiores del modelo OSI.

Esta tesis presenta un sistema de Seguridad en Capa Física considerando como escenario un sistema de comunicaciones que emplea el estándar IEEE 802.11a en presencia de un espía. El sistema propone el uso de la Descomposición Algebraica de Canal, el cual es único entre el transmisor y el receptor legítimo, éste provee la clave de seguridad a través del uso de las matrices U_k, Δ_k y V_k obtenidas al realizar tal proceso. La matriz V_k es la que multiplica a los símbolos OFDM, siendo esta la matriz que encripta los datos, en tanto, en el receptor se tiene a las matrices U_k, Δ_k que representan las matrices desencriptadoras. Por otro lado, el espía, quien posee un canal de propagación distinto, no podrá desencriptar los datos que se transmiten. El nivel de seguridad se mide a través de los altos niveles obtenidos de BER (Bit Error Rate) del atacante en comparación del receptor legítimo.

Las simulaciones realizadas se presentan en dos escenarios. El primer escenario es cuando el espía no tiene conocimiento de su canal de propagación e intenta realizar la desencriptación de los símbolos enviados entre el transmisor y receptor legítimo. Para ello se transmiten 1000 símbolos OFDM cada uno compuesto de 52 subportadoras de datos modulados con BPSK (Binary Phase Shift Key), esto basado en el estándar IEEE 802.11a. Para este caso, el BER obtenido es casi constante de $10^{-0.3}$ para el espía con distintos valores de E_b/N_o, en tanto que para el receptor legítimo los valores de BER caen conforme el E_b/N_o se incrementa. El segundo escenario se presenta cuando el espía tiene conocimiento de su canal de propagación y del mismo modo realiza la desencriptación de los símbolos. Al igual que el caso anterior, los valores de BER que obtiene el espía siguen siendo casi constantes $10^{-0.3}$ para distintos valores de E_b/N_o.

1. Introducción

En los últimos años, las tecnologías inalámbricas han tenido un gran impacto en la sociedad, ya que a través de ellas las personas pueden estar comunicadas en cualquier momento y en cualquier lugar, teniendo como resultado el uso masivo de éstas por sobre las tecnologías alámbricas. Es por ello que surge la necesidad de optimizar los servicios ofrecidos, lo cual se ha traducido en la constante investigación e innovación. Entre los avances tecnológicos desarrollados se encuentran: La codificación adaptativa, MIMO (Multiple Input Multiple Output) y la mejora en la eficiencia del espectro gracias a OFDM (Orthogonal Frecuency Division Multiplexing), logrando incrementar la tasa de transmisión por usuario sin comprometer la calidad de servicio.

Sin embargo, asi como las tecnologías inalámbricas traen consigo importantes innovaciones al mismo tiempo presentan problemas relacionados al tema de seguridad, debido a que la información se transmite por medio de ondas electromagnéticas que viajan por el espacio libre, de manera que cualquier individuo equipado con las características adecuadas podría recibir la señal y analizarla. Por tal motivo, desarrollar mecanismos robustos y eficientes que protejan la información que se transmite es de vital importancia, para tal efecto se debe tener en consideración dos características principales. La primera de ellas es la fiabilidad del sistema, los mensajes enviados a un usuario específico (receptor legítimo) deben ser interpretada de manera correcta por tal usuario, lo cual representa que el error de decodificación del sistema deba satisfacer una especificación dada. La segunda es el secreto del mensaje, bajo ciertas condiciones, un transmisor puede enviar mensajes a un receptor legítimo en presencia de un individuo que está escuchando la transmisión, y éste no sea capaz de entender la información enviada.

Este trabajo presenta un Sistema de Seguridad en Capa Física aplicado al estándar Wi-Fi 802.11a en banda base que utiliza OFDM, el sistema se basa en la Descomposición Algebraica del Canal de Comunicación como clave de seguridad entre un transmisor y receptor legítimo, consiguiendo que un espía, que escucha la comunicación y no tiene conocimiento sobre el canal, sea incapaz de desencriptar la información. Esto queda demostrado cuando el espía obtiene niveles elevados de BER (Bit Error Rate) para diferentes valores de E_b/N_o en comparación del receptor legítimo.

1.1. Motivación y Contexto

La seguridad en redes inalámbricas es tema de constante desarrollo por los investigadores y empresas que día a día tienen que lidiar para contrarrestar los diversos ataques que se presentan contra la información. Conforme han pasado los años, se han trabajado innumerables técnicas que han servido como soluciones momentáneas hasta que aparecen nuevos mecanismos que vulneran la seguridad de los sistemas, ocasionando que nuevas técnicas se implementen. Un caso en particular es el que presenta el estándar IEEE 802.11, el cual ha venido mejorando sus mecanismos de seguridad, entre los que destacan: WEP (Wired Equivalent Privacy) , WPA (Wi-Fi Protected Access), WPA2 (Wi-Fi Protected Access 2), las cuales son técnicas que se enfocan a la encriptación de datos a nivel de capa de enlace, ofreciendo un nivel mayor de seguridad en la comunicación. Sin embargo, las nuevas soluciones apuntan al uso de la capa física para el desarrollo de mecanismos que incrementen el nivel de seguridad. Por tanto, es importante implementar un mecanismo de seguridad sobre capa física, aplicando técnicas directamente sobre la modulación, codificación y canal de comunicación, para asi reforzar el nivel de seguridad actual.

1.2. Planteamiento del problema

En años recientes hemos sido testigos del crecimiento de ataques en diversas redes de telecomunicaciones, la mayor parte de estos ataques han sido realizados sobre redes inalámbricas, esto debido a la naturaleza de libre acceso del medio de transmisión. Por lo que nadie está exento a este hecho, y tal es el caso de empresas que invierten grandes cantidades de dinero para proteger su información, y los millones de usuarios que hacen uso de estas redes.

Según el Director Nacional de Inteligencia de Estados Unidos, en el año 2014, los delitos contra la seguridad informática están clasificados como las principales amenzas a la seguridad nacional por encima del terrorismo, el contrabando de armas, entre otros [Mic14], y se prevé que este comportamiento siga siendo el mismo para los próximos años. Frente a ello, diversas organizaciones a nivel mundial han venido desarrollando mecanismos criptográficos como es el caso del IEEE a través de sus estándares 802.11 y 802.16 en sus diversas versiones, pero esto no ha sido suficiente para contar con servicios seguros en la comunicación.

Por lo tanto, de no incrementar el nivel de seguridad actual, ello conducirá a innumerables pérdidas de dinero y de tiempo por parte de las empresas y de los usuarios, además que el uso masivo de esta tecnología se vería afectado por no contar con mecanismos robustos de seguridad.

1.3. Objetivos

1.3.1. Objetivo general

Desarrollar un método de encriptación de datos a nivel de capa física empleando Descomposición Algebraica del Canal entre el Transmisor y el Receptor Legítimo para Comunicaciones Inalámbricas OFDM.

1.3.2. Objetivos específicos

1. Analizar los estimadores de canal LSE y MMSE y elegir el más adecuado para su aplicabilidad desde el punto de vista de seguridad.
2. Lograr que la probabilidad de error para el atacante presente niveles constantes para diferentes valores de E_b/N_o con el método propuesto.
3. Analizar los mecanismos de seguridad en capa física y comparar con el propuesto en términos de BER para el atacante y el receptor legítimo.

1.4. Organización del trabajo

El presente documento consta de seis capítulos. El primer capítulo está dedicado a la introducción del trabajo de tesis, donde se presenta una vista general sobre el impacto de las comunicaciones inalámbricas OFDM y sus problemas de seguridad.

En el segundo capítulo se desarrolla el marco teórico, aquí se presenta los conceptos relacionados a las redes inalámbricas, la capa física, la descomposición algebraica, el canal de propagación, los algoritmos que se utilizan para realizar la estimación de canal y finalmente OFDM.

En el tercer capítulo se desarrolla el estado del arte, donde se describen algunas de las técnicas que se han venido desarrollando en capa física para mejorar el nivel de seguridad en las comunicaciones inalámbricas.

En el cuarto capítulo se describe la solución propuesta a nuestro problema de forma detallada.

En el quinto capítulo se presenta las simulaciones y resultados de la solución propuesta. El software utilizado para dichas simulaciones es MATLAB R2009a.

En el sexto capítulo se presentan las conclusiones del presente trabajo, así como los posibles trabajos futuros.

2. Marco Teórico

En este capítulo se presentan una serie de conceptos que ayudarán a comprender las bases de esta investigación. En la Sección 2.1 se mencionan los tipos, la arquitectura y la seguridad que presentan las redes inalámbricas. La descripción de la capa física basado en el estándar IEEE 802.11 es presentado en la Sección 2.2. El concepto y los tipos de descomposición algebraica son expuestos en la Sección 2.3. El canal de propagación y sus modelos son mencionados en la Sección 2.4. La Sección 2.5 explica los distintos algoritmos que se utilizan para realizar la estimación de canal. Por último, en la Sección 2.6 se detalla la multiplexación por división de frecuencia ortogonal, conocido como OFDM, su uso, ventajas y desventajas que trae consigo.

2.1. Redes Inalámbricas

Las redes inalámbricas consisten en la transmisión y recepción de información a través de ondas electromagnéticas que viajan por medio de la interfaz aérea [Dez07]. Este tipo de redes presenta algunas ventajas respecto a las tradicionales redes cableadas, entre las que se tiene: La ausencia de cableado ofrece movilidad a los usuarios, la flexibilidad en la topología de la red y escalabilidad. Sin embargo, también presentan algunos inconvenientes como son el menor ancho de banda, la seguridad y garantizar ciertos niveles de QoS (Quality of Service).

2.1.1. Clasificación de Redes Inalámbricas basado en cobertura

Existen diferentes tipos de redes inalámbricas que son usadas hoy en día. A continuación se realiza una breve descripción:

- WPAN (Wireless Personal Area Network) o redes inalámbricas de área personal. Presentan coberturas menores a 10 metros, es usado para interconectar dispositivos personales.

- WLAN (Wireless Local Area Network) o redes inalámbricas de área local. Cubren alrededor de 100 metros y son utilizadas para crear redes de ámbito local.

- WMAN (Wireless Metropolitan Area Network) o redes inalámbricas metropolitanas. Su área de cobertura pretende cubrir una ciudad o población.

- Redes globales. Este tipo de redes son las redes celulares en sus diferentes tecnologías GSM, UMTS, HSDPA, LTE.

En la Figura 2.1 se muestra la evolución que han tenido las diferentes tecnologías inalámbricas respecto a la velocidad de datos y el área de cobertura.

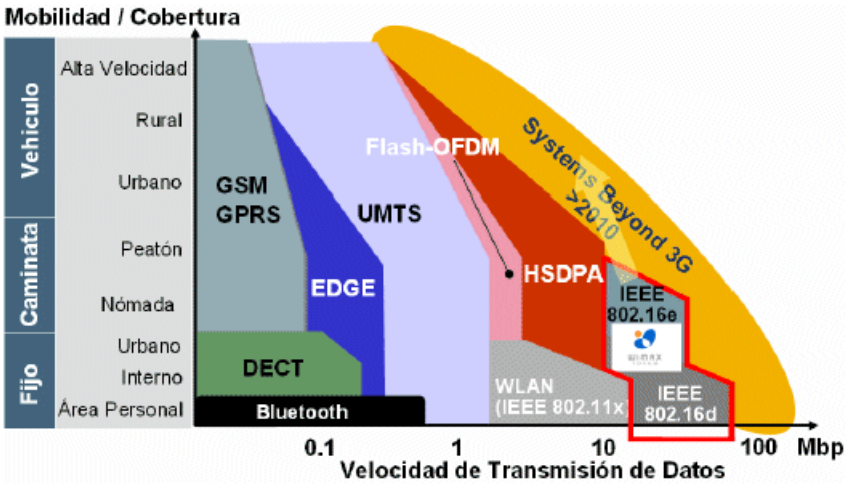

Figura 2.1.: Velocidad de Transmisión y Movilidad de las Tecnologías Inalámbricas. [LDRV07]

2.1.2. Arquitectura de Redes Inalámbricas

La arquitectura de una red inalámbrica determina cómo está estructurada y dónde reside el control de esta. En [Dez07] menciona que se pueden diferenciar dos tipos de arquitecturas de redes inalámbricas: Centralizadas y distribuidas.

2.1.2.1. Redes Inalámbricas Centralizadas

Tal como se muestra en la Figura 2.2 está conformada por dispositivos inalámbricos que se conectan a un único punto de acceso, quien se encarga de coordinar y controlar todas las transmisiones que se realizan dentro de su área de cobertura.

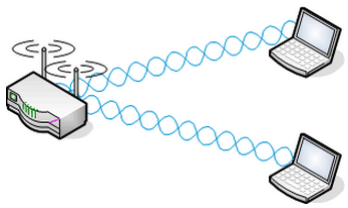

Figura 2.2.: Arquitectura Inalámbrica Centralizada. [Dez07]

2.1.2.2. Redes Inalámbricas Distribuidas

De acuerdo a [Dez07, CM09] las redes inalámbricas distribuidas son aquellas en la que todos los dispositivos inalámbricos proporcionan servicios de enrutamiento, además retransmiten la información entre aquellos que no tienen una conexión directa, esto se muestra en la Figura 2.3.

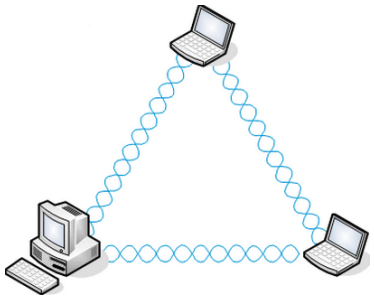

Figura 2.3.: Arquitectura Inalámbrica Distribuida. [Dez07]

2.1.3. Seguridad en Redes Inalámbricas

De acuerdo a [Str04, Gar10, Her], seguridad es toda aquella acción que tiende a garantizar el cumplimiento de cuatro objetivos importantes: Confidencialidad, integridad, disponibilidad y autentificación, todos ellos definidos por el estándar X.800 [ITU91]. Tales definiciones se presentan a continuación:

- Confidencialidad: La información no esté disponible a personas y procesos no autorizados.
- Integridad: Los datos no hayan sido cambiados de manera accidental o no autorizada.
- Disponibilidad: La información debe ser accesible en cualquier momento.
- Autentificación: Verificar la identidad del emisor y del receptor.

Así mismo, los autores [Paz11, QP08, GA04] describen los protocolos en seguridad inalámbrica definidos para el estándar IEEE 802.11. A continuación se detallan cada uno de ellos.

2.1.3.1. WEP (Wired Equivalent Privacy)

WEP fue el primer protocolo de encriptación introducido por el estándar IEEE 802.11a, tiene como finalidad proteger la confidencialidad y la integridad. Está basado en el algoritmo de clave simétrica RC4 (River Cipher 4), éste algoritmo consiste en expandir la clave compartida, la cual debe de ser conocida tanto por el transmisor como por el receptor, generándose un flujo de bits pseudoaleatorios llamados key

stream. Para cifrar el mensaje se realiza la operación XOR entre el key stream y el mensaje a enviar. Para recuperar el mensaje se vuelve a realizar la operación XOR entre el cipher stream recibido y el key stream generado.

Entre las debilidades de WEP se encuentran:

- Uso de claves estáticas.
- Todos los usuarios tienen la misma clave.
- En caso la clave sea modificada, la actualización de la clave ha de realizarse de manera manual en cada dispositivo.

2.1.3.2. WPA (Wi-Fi Protected Access)

Debido a las debilidades que presentó WEP, Wi-Fi Alliance propuso dos nuevas versiones, estas fueron WPA y WPA2. La gran diferencia de estos protocolos es el cifrado que utilizan: WPA usa TKIP (Temporary Key Integrity Protocol) basado en RC4, en tanto WPA2 utiliza CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol) basado en AES (Advanced Encryption Standard).

A diferencia de WEP que utilizaba la misma clave para toda la red inalámbrica, en WPA las claves son generadas y distribuidas cada intervalo de tiempo por el AP o por un servidor RADIUS (Remote Authentication Dial In User Service) de autenticación. Además presenta una mejora respecto a la integridad de la información cifrada, ya que en lugar de utilizar la comprobación de redundancia cíclica utiliza un código de integridad de mensaje.

2.1.3.3. WPA2 (Wi-Fi Protected Access 2)

WPA2 es utilizado en el nuevo estándar 802.11i, utiliza el protocolo CCMP reemplanzado el código de integridad de mensaje utilizado en WPA con lo cual asegura la integridad de los mensajes, además la encriptación mejora con AES en lugar de RC4.

2.1.4. Vulnerabilidades en Redes Inalámbricas

Debido que las redes inalámbricas utilizan el espectro electromagnético para enviar/recibir información, estas traen consigo una serie de vulnerabilidades. A continuación se describen algunas de ellas.

2.1.4.1. Eavesdropping (Escucha sin Autorización)

Según [Bat09, MMA07], este tipo de vulnerabilidad consiste en obtener información que es normalmente transmitida por la red, tales como: los nombres de usuarios, las contraseñas, las direcciones IP, entre otros. En Internet esto es realizado por packet sniffers, que son programas que monitorizan los paquetes que circulan por la de red. Para contrarrestar tal ataque, se usa el cifrado de datos a nivel de capa de transporte. En muchos casos en lugar de utilizar TCP, se usa SSL (Secure Socket Layers), SSH (Secure Shell) o IPSec, los cuales son protocolos que utilizan cifrado para transportar datos sensibles. Entonces, un atacante puede capturar los datos cifrados, pero éstos no serían válidos debido a que el atacante no podría descifrar su contenido.

2.1.4.2. Spoofing (Suplantación de Identidad)

Los autores en [MMA07] señalan que esta técnica es utilizada para suplantar la identidad de usuarios autorizados. Existe diferente tipos de spoofing, tales como el IP spoofing, el atacante genera paquetes de Internet con una dirección de red falsa en el campo origen, pero que es aceptada por el destinatario del paquete. Existen algunos mecanismos para combatir tal ataque, uno de ellos es que se usen certificados de seguridad para que sólo puedan acceder a la red usuarios legítimos, pero el coste computacional crece. El ARP spoofing es otro tipo conocido que consiste en modificar la tabla ARP de una victima con el fin de que envíe paquetes al atacante en lugar del receptor legitimo.

2.1.4.3. Denial of Service (Denegación de Servicios)

Este tipo de ataque hace que los clientes no consigan acceder a la red, la técnica se basa en enviar tramas erróneas al medio, de modo que se degrade el servicio que se ofrece. Además, existen otras maneras de provocar un ataque de Denegación de Servicio utilizando dispositivos que saturen la banda de frecuencias en la que trabajan los dispositivos inalámbricos.

2.2. Capa física

El objetivo de la capa física en una red inalámbrica consiste en representar los bits de las tramas de la capa de enlace de datos en señales electromagnéticas.

2.2.1. Descripción de la capa física basado en el estándar IEEE 802.11

En el estándar IEEE 802.11 [IEE03] se detallan las funciones que realiza la Capa de Enlace y la Capa Física, esto se muestra en la Figura 2.4.

La capa MAC (Medium Access Control) se encarga de:

- Controlar el acceso al medio.

- Fragmentación, desfragmentación y encriptado.

- Gestión de potencia, sincronización y escaneo del medio.

- Control de flujo y el manejo de múltiples tasas de transmisión.

Figura 2.4.: Pila de Protocolos del Estándar IEEE 802.11. [Esp11]

Así mismo, para el control de acceso al medio, el estándar utiliza el protocolo CSMA/CA (Carrier Sense Multiple Access/ Collision Avoidance), en el que se realiza las siguientes funciones [Bat09]:

- Una estación mide el nivel de señal antes de transmitir para determinar su estado (libre/ocupado).

- Si el medio no está ocupado por otra trama, la estación hace una espera adicional llamada IFS (Interframe Space).

- Si durante este intervalo, el medio se considera ocupado, la estación debe esperar hasta el final de la transmisión actual.

La subcapa MAC obtiene las MSDU (MAC Service Data Unit) o las MMPDU (MAC Management Protocol Data Unit) procedentes del subnivel LLC (Logical Link Control) y las fragmenta, en la Figura 2.5 se muestra tal proceso.

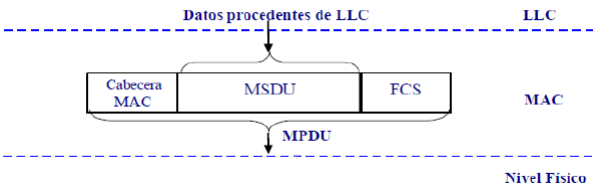

Figura 2.5.: Encapsulado en la Capa MAC. [Esp11]

En [IEE03, Esp11, Bat09], se menciona que la capa física está dividida en dos subcapas: PLCP (Physical Layer Convergence Protocol) y PMD (Physical Medium

Dependent). La subcapa PMD se encarga de la transmisión de las tramas. En tanto, la subcapa PLCP es la interfaz entre la subcapa MAC y la capa Física y proporciona el mecanismo de detección de portadora y la CCA (Clear Channel Assessment). El CCA es una señal que la capa MAC tiene que identificar para determinar si el canal está libre u ocupado. El encapsulado que se realiza a nivel de capa físico se muestra en la Figura 2.6.

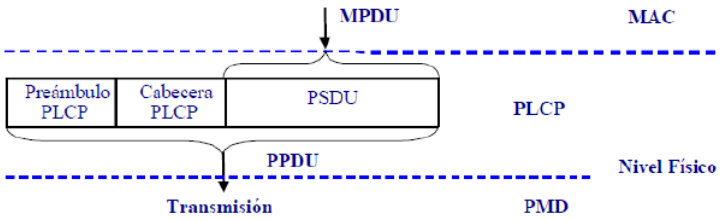

Figura 2.6.: Encapsulado en la Capa Física. [Esp11]

En el proceso de transmisión, la subcapa MAC indica a la subcapa PLCP que prepare MPDUs. Del igual manera, en el proceso de recepción, la subcapa PLCP ofrece tramas de entrada del medio inalámbrico a la subcapa MAC. Bajo la dirección de la subcapa PLCP, la subcapa PMD proporciona transmisión y recepción de unidades de datos de capa física entre dos estaciones a través del medio inalámbrico y ofrece modulación y demodulación de las transmisiones de la trama. Los tipos de modulaciones y codificaciones dependerán de los protocolos existentes en éste estándar.

A continuación se mencionan las modulaciones y codificaciones utilizados en tres protocolos del estándar IEEE 802.11:

IEEE 802.11b

- Modulación DBPSK para 1Mbps
- Modulación DQPSK para 2Mbps
- Modulación CCK (Complementary Code Keying) para 5.5 y 11 Mbps.

IEEE 802.11a

- OFDM a una frecuencia de 5 GHz
- Velocidades de datos de 6, 9, 12, 18, 24, 36, 48 y 54 Mbps.
- 52 sub-portadoras moduladas BPSK, QPSK, 16QAM ó 64QAM.
- Codificadores convolucionales con una tasa de 1/2, 2/3, o 3/4.

IEEE 802.11g

- OFDM a una frecuencia de 2,4 GHz
- Velocidades de datos de 6, 9, 12, 18, 24, 36, 48 y 54 Mbps.

- 52 sub-portadoras moduladas BPSK, QPSK, 16QAM ó 64QAM
- Codificadores convolucionales con una tasa de 1/2, 2/3, o 3/4.

2.3. Descomposición Algebraica

En este apartado se repasa algunas de las técnicas utilizadas para la descomposición algebraica de matrices, es decir, técnicas que nos permiten escribir una matriz como producto de dos o tres matrices con una estructura especial. Entre ellas tenemos la descomposición LU, la descomposición QR, y finalmente la descomposición SVD (Single Value Descomposition).

2.3.1. Descomposición LU

La descomposición LU está directamente relacionada con las operaciones elementales aplicadas a una matriz, para llevarla a una forma triangular inferior [Vie]. Supongamos que se conoce cómo descomponer una matriz A de dimensiones $m \times n$.

$$A = LU \tag{2.1}$$

Donde L es una matriz triangular inferior de dimensiones $m \times m$ y U es una matriz escalonada de dimensiones $m \times n$. Entonces un sistema de la forma:

$$Ax = b \tag{2.2}$$

Puede resolverse de la siguiente forma:

$$L(Ux) = b \tag{2.3}$$

Si aplicamos un cambio de variable: $y = Ux$, tenemos:

$$Ly = b \tag{2.4}$$

Resolvemos entonces dicho sistema para la variable y; mediante sustitución hacia adelante. Como paso final, usamos sustitución hacia atrás para resolver el sistema

$$Ux = y \tag{2.5}$$

2.3.2. Descomposición QR

Esta sección describe la descomposición QR de una matriz. Dicha descomposición es de gran importancia para resolver problemas de mínimos cuadrados y tiene una estrecha relación con el cálculo de la inversa generalizada de una matriz [Gar].

Teorema:

Si A es una matriz de dimensiones $m \times n$ con columnas linealmente independientes, entonces A puede factorizarse en la forma:

$$A = QR \tag{2.6}$$

En la que Q es una matriz con columnas ortonormales de dimensiones $m \times m$ y R es una matriz triangular superior de dimensiones $m \times n$.

Demostración:

Sean: $a_1, a_2, ..., a_n$ las columnas de A y sean $q_1, q_2, \ldots, q_n$ los vectores obtenidos utilizando el proceso de ortogonalización Gram-Schmidt.

Definamos: $Q = [q_1, q_2, ..., q_n]$

Como cada a_i es combinación lineal de $q_1, q_2, \ldots, q_n$ deben existir escalares r_{ij} tales que:

$$a_i = r_{1i}q_1 + ... + r_{ni}q_n \tag{2.7}$$

$$a_i = r_{1i}q_1 + ... + r_{ni}q_n = Q \begin{bmatrix} r_{1i} \\ . \\ . \\ r_{ni} \end{bmatrix} \; i = 1, 2, 3...n \tag{2.8}$$

Finalmente la matriz R puede ser calculada de la siguiente manera:

$$R = Q^T A \tag{2.9}$$

2.3.3. Descomposición SVD

En [Gar, VM] se menciona que la descomposición SVD se basa en la determinación de que cualquier matriz A de dimensiones $m \times n$ puede ser escrita como el producto de: Una matriz U con columnas ortogonales de dimensiones $m \times n$; una matriz diagonal W de $n \times n$ con elementos positivos o ceros, los cuales son los valores singulares de A; y por la transpuesta de una matriz V de dimensiones $n \times n$.

Definición: Sean m, n enteros positivos y una matriz $A \in C^{m \times n}$. Una descomposición en valores singulares de A:

$$A = UWV^T \tag{2.10}$$

Donde: $U \in C^{m \times n}$ y $V \in C^{m \times n}$. Además:

$$W = \begin{cases} \begin{bmatrix} Diag(\sigma_1, \ldots, \sigma_n) \\ 0_{m-n\,x\,n} \end{bmatrix} si\, m \geq n \\ [Diag(\sigma_1, \ldots, \sigma_n)\ 0_{m\,x\,n-m}]\, si\, m \leq n \end{cases} \tag{2.11}$$

En cualquier caso, $\sigma_1 \geq \ldots \geq \sigma_s \geq 0$, $s = min\{m, n\}$, son números reales no negativos ordenados de mayor a menor y se llaman valores singulares de A. Además, a los vectores $\mu_1, \ldots, \mu_m$ y $v_1, \ldots, v_m$, los cuales conforman las columnas de U y V se le llama vectores singulares de A por la izquierda y por la derecha, respectivamente.

2.4. Canal de propagación

En las redes inalámbricas la energía que envia una trasmisor atraviesa diversos caminos para llegar al receptor, el conjunto de estos caminos es llamado canal multicamino o de propagación. Cada camino se puede caracterizar en función del tiempo, la intensidad y la variación en fase con la que llegan a su destino. El tiempo de llegada de cada camino es denominado retraso temporal, éste depende de la distancia y la velocidad a la que se propague la onda, mientras que la intensidad o atenuación de amplitud y el cambio de fase dependen de los objetos sobre los cuales la onda es reflejada[Pol11]. En la Figura 2.7 se presenta un ejemplo de la propagación multicamino que sufren las señales para llegar a su destino.

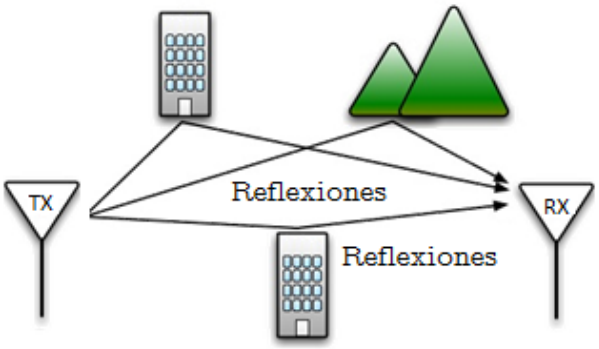

Figura 2.7.: Propagación multicamino [Pol11]

El objetivo ahora es modelar el canal multicamino en función de la amplitud, el retardo y la fase. En primer lugar asumiendo que las diferencias temporales son despreciables respecto al período de la señal transmitida, entonces el efecto de retardo es el mismo en todas las frecuencias [Agu01]. Si se considera que el número de caminos que llegan al receptor es grande, se puede tratar las componentes en fase h_f y cuadratura h_c del canal como Variables Aleatorias Gaussianas con varianza σ, donde cada camino sigue una Función de Densidad de Probabilidad dada por:

$$p_H(h) = \frac{1}{2\pi\sigma^2} e^{-\left(\frac{h_f^2+h_c^2}{2\sigma^2}\right)} \tag{2.12}$$

Ahora bien, si existe línea de vista directa, entonces la señal recibida se compone de múltiples ondas reflejadas y una onda con nivel de señal mayor, a esta componente aleatoria debe añadirse una componente determinista, de manera que la Función de Densidad de Probabilidad Gaussiana presenta media distinta de cero y varianza σ:

$$p_H(h) = \frac{1}{2\pi\sigma^2} e^{-\left(\frac{(h_f+m_f)^2+(h_c+m_c)^2}{2\sigma^2}\right)} \tag{2.13}$$

La envolvente del canal, $r = |h|$, es la raíz cuadrada de la suma de los cuadrados de dos gaussianas de igual varianza, por lo que la envolvente de la señal recibida se puede modelar como una Distribución de Rice, que viene dado por:

$$p_r(r) = \frac{1}{\sigma^2} e^{-\left(\frac{r^2+r_s^2}{2\sigma^2}\right)} I_0\left(\frac{r.r_s}{\sigma^2}\right) \tag{2.14}$$

Donde $I_0(\bullet)$ es la función de Bessel modificada de primera especie y de orden cero y r_s es la envolvente de la componente directa.

Para el caso de no tener línea de visión directa, donde todas las ondas incidentes han sido reflejadas al menos una vez, y la envolvente de la señal recibida se puede modelar mediante una Distribución de Rayleigh, que viene dado por:

$$p_r(r) = \frac{1}{\sigma^2} e^{-\left(\frac{r^2}{2\sigma^2}\right)} \tag{2.15}$$

Finalmente, la respuesta impulsional del canal multicamino, $h(\tau, t)$se puede define como la respuesta del canal en tiempo t debida a un impulso aplicado en el instante $t - \tau$:

$$h(\tau; t) = \sum_n a_n(t)\, e^{-j2\pi f_c \tau_n(t)} .\delta[\tau - \tau_n(t)] \tag{2.16}$$

Donde: $a_n(t)$ es la atenuación de la señal recibida en el camino n-ésimo en el instante t, $\tau_n(t)$ es el retardo de la señal por el camino n-ésimo en el instante t, $e^{-j2\pi f_c \tau_n(t)}$es la rotación de fase por el camino n-ésimo en el instante t a la frecuencia portadora f_c.

2.5. Estimación de canal

Conocer la respuesta del canal multicamino en comunicaciones inalámbricas permitirá procesar la señal recibida de manera más óptima, para ello, una herramienta que se usa para tal fin son los algoritmos de estimación de canal. En [Cor09] se menciona que el funcionamiento básico de los algoritmos de estimación de canal en OFDM comienza en el transmisor, ya que éste incluye cierta información en los datos que se envía, con lo que existe la posibilidad de incluir cierta información adicional o no estableciendo si se trata de un algoritmo de estimación mediante secuencias de entrenamiento o ciego.

Típicamente en los sistemas OFDM utilizan la técnica de estimación de canal conocida como PSAM (Pilot Symbol Assisted Modulation), el cual consiste en adicionar simbolos pilotos sobre la información a transmitir. Al atravesar el canal, éste afectará los datos incluidos por el transmisor de la misma manera que la información principal. Al llegar al receptor se demodula la señal y se extrae la información transmitida. De esta forma el receptor, a partir de los símbolos de entrenamiento recibidos y su conocimiento sobre los que fueron transmitidos tratará de estimar cuál ha sido el comportamiento del canal durante esa transmisión. En la Figura 2.8 se presenta el diagrama de bloques de un receptor OFDM que usa esta técnica.

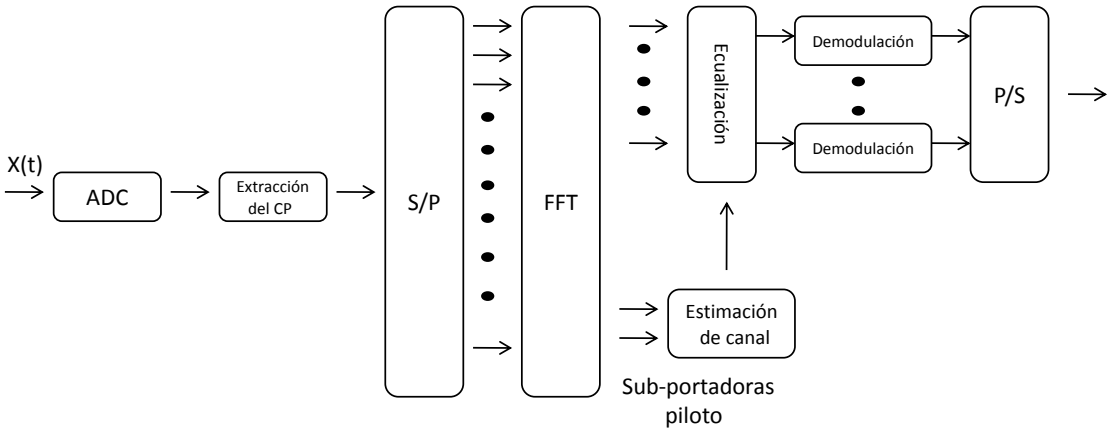

Figura 2.8.: Diagrama de Bloques de Receptor OFDM en Banda Base. [Cor09]

2.5.1. Estimación asistida por datos

Los algoritmos de estimación basados en secuencias de entrenamiento consisten en la inserción de datos en un conjunto de subportadoras de la señal a transmitir. De acuerdo a [Pol11], el proceso de estimación de canal consiste en una comparación por parte del receptor entre lo que llega y lo que debería llegar observando la distorsión sufrida por la señal a causa del canal y del ruido presente. Este ruido implica una degradación en la estimación de canal, es por ello que se requiere tener una buena SNR. Para conseguir la mayor SNR posible se escogen como símbolos piloto aquellos que tenga mayor energía. Sin embargo, existe la contraparte que la tasa de información a transmitir se ve reducida dado que es necesario destinar cierta capacidad para transmitir periódicamente la secuencia de entrenamiento.

2.5.2. Estimación no asistida por datos

El modelo básico de estimación del canal no asistida por datos, también conocida como ciega, se muestra en la Figura 2.9, donde solo la señal recibida es accesible para la identificación y estimación del canal H.

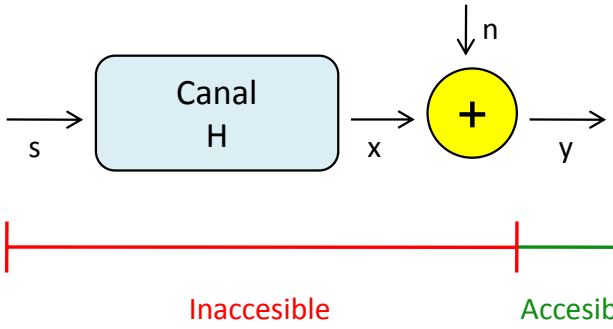

Figura 2.9.: Modelo de Estimación no Asistida por Datos. [Pol11]

La esencia de la estimación ciega de canal se basa en el conocimiento de algunas propiedades de la señal de entrada, como lo es un distribución de probabilidad conocida o un alfabeto finito conocida de simbolos. A pesar de ello, los estándares IEEE 802.11, IEEE 802.16 no utilizan estos algoritmos de estimación de canal.

En el Cuadro 2.1 se realiza una comparativa entre los dos algoritmos descritos.

2.5.3. Técnicas de Estimación de Canal

La estimación de canal en OFDM es un tema sobre el que ha surgido un gran interés en la última década. Todas estas técnicas parten del cálculo de las estimaciones del canal en las posiciones piloto [Cor09].

Algoritmos asistidos por datos	Algoritmos no asistidos por datos
Secuencia de entrenamiento conocido por el Rx.	No son necesarias secuencias de entrenamiento.
Fácil de implementar.	Difícil de implementar en sistemas de tiempo real
Baja carga computacional	Alta carga computacional
Desperdicio de ancho de banda de transmisión	Aplicable en sistemas con ancho de banda estrecho

Cuadro 2.1.: Características de los Algoritmos de Estimación de Canal

A continuación se describen los estimadores de canal. El primero de ellos es el conocido como Estimador de Máxima Verosimilitud, el cual define una función estadística, donde ésta función se construye a partir de variables observadas. Luego, se desarrollan dos tipos de estimadores, LSE y MMSE, los cuales tienen como objetivo de diseño minimizar el error de detección.

2.5.3.1. Estimador ML (Maximum Likelihood)

En [Mia06] se desarrolla este tipo de estimador, el cual considera un modelo de canal h, donde se asume que es un canal en tiempo discreto con respuesta al impulso finito de orden L.

$$h = \{h[1], h[2], \ldots, h[L]\}^T \tag{2.17}$$

Además supongamos que se tiene N muestras recibidas

$$y = \{y[0], y[1], \ldots, y[N-1]\}^T \tag{2.18}$$

Por lo que, tenemos el siguiente modelo lineal dado por:

$$y = Sh + z \tag{2.19}$$

Donde S es una matriz Toeplitz de dimensiones $N \times L$, la cual consiste de las muestras de la secuencia de entrada $s[n]$ dada por:

$$S = \begin{bmatrix} s[0] & s[N-1] & \ldots & s[N-L+1] \\ s[1] & s[0] & \ldots & s[N-L+2] \\ \vdots & \vdots & \ddots & \vdots \\ s[N-1] & s[N-2] & \ldots & s[0] \end{bmatrix} \tag{2.20}$$

Y z es un vector de ruido dado por:

$$z = \{z[0], z[1], \ldots z[N-1]\}^T \tag{2.21}$$

Sea θ el vector de parámetros desconocidos, el cual puede contener el canal h. Asumimos que el vector de ruido z como el vector de entrada s, son conocidos. Entonces es posible obtener la función de densidad de probabilidad conjunta del vector de observación y, el cual se escribe como $f_y(y;\theta)$, a esta función se denomina función de máxima verosimilitud. Esta función de máxima verosimilitud está dado por:

$$f_y(y;\theta) = f(y[0],\theta)\, f(y[1],\theta) \ldots f(y[N-1],\theta) \tag{2.22}$$

Entonces, el Estimador de Máxima Verosimilitud es la solución de la siguiente ecuación:

$$\frac{df_y(y;\theta)}{d\theta} = 0 \tag{2.23}$$

Así mismo, la función de densidad de probabilidad conjunta puede ser reescrita de la siguiente forma debido a que las muestras observadas son *iid* (independiente e idénticamente distribuida).

$$f_y(y;\theta_1,\theta_2,\ldots\theta_k) = \prod_{n=0}^{N-1} f_{y[n]}(y[n];\theta_1,\theta_2,\ldots\theta_k) \tag{2.24}$$

El Estimador de Máxima Verosimilitud usualmente tiene un buen rendimiento cuando el tamaño de la observación es suficientemente largo, pero su implementación es computacionalmente cara.

2.5.3.2. Estimador LSE (Least Square Error)

En [Cor09, Mia06] se desarrolla este tipo de estimador, donde se considera el canal en tiempo discreto visto en la sección anterior. Además se tiene las muestras recibidas y, descrita por:

$$y = Sh + z \tag{2.25}$$

Donde S es una matriz conocida de orden $N \times L$ y z es el vector de ruido. Así mismo, se asume que el vector de ruido no es normalmente distribuida y tiene media $E\{z\} = 0$ y covarianza $V\{z\} = \Omega$. Por otro lado, cuando en el modelo de canal discreto la función de densidad de probabilidad conjunta de las variables aleatorias observadas no es dada, entonces la estimación del canal h se puede hallar usando el método de Mínimos Cuadrados.

Por lo tanto, se plantea lo siguiente, se escoge los valores de h que minimicen la suma residual de los cuadrados, para ello aplicamos la primera derivada respecto h e igualamos a 0.

$$L\left(y;h\right)=\left(y-Sh\right)^{T}\left(y-Sh\right) \tag{2.26}$$

$$\frac{dL\left(y;h\right)}{dh}=-S^{T}\left(y-Sh\right)-\left(y-Sh\right)^{T}S=0 \tag{2.27}$$

$$\frac{dL\left(y;h\right)}{dh}=-2S^{T}\left(y-Sh\right)=0 \tag{2.28}$$

$$\hat{h}=\left(S^{T}S\right)^{-1}S^{T}y \tag{2.29}$$

2.5.3.3. Estimador MMSE (Minimum Mean Square Error)

En esta sección se presenta una solución lineal óptima, la cual es conocida como el estimador MMSE basada en el filtro de Wiener. El principal resultado es derivar las ecuaciones de Wiener-Hopf que proveen los coeficientes del filtro óptimo FIR (Finite Impulse Response) para la estimación del canal [Mia06]. En la Figura 2.10 se muestra el diagrama de bloques del estimador MMSE. Como se aprecia $d\left[n\right]$ es la respuesta estimada de $y\left[n\right]$, para lograr la estimación se necesita tener dos procesos estacionarios en sentido amplio, $s\left[n\right]$ y $y\left[n\right]$, los cuales son estadísticamente relacionados uno con otro. Así mismo tenemos que asumir que las funciones de autocorrelación $r_{s}\left(k\right)$y $r_{y}(k)$, y la función de correlación cruzada $r_{ys}\left(k\right)$, son conocidas.

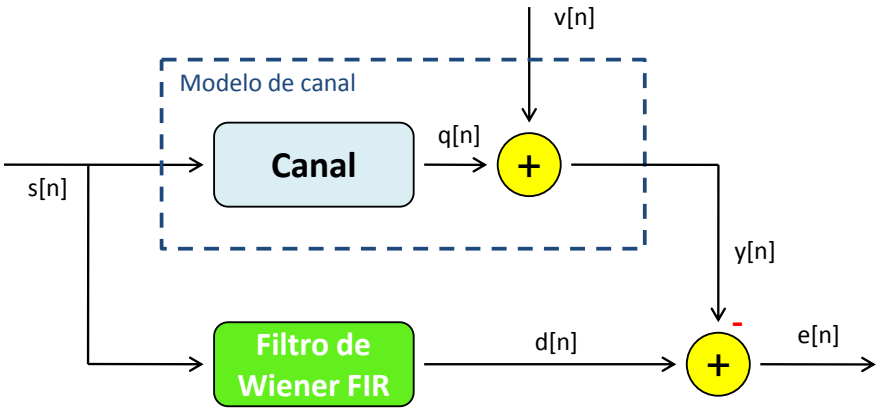

Figura 2.10.: Estimador MMSE basado en la Solución Wiener-Hopf. [Mia06] [20]

Ahora bien, para desarrollar el estimador MMSE, se tiene que determinar los coeficientes del filtro FIR, $w\left[n\right]$, el cual minimiza el error cuadrático medio de la salida del filtro $d\left[n\right]$ comparado con la salida del modelo de canal $y[n]$. Entonces el objetivo es minimizar el error que viene dado de la siguiente manera:

$$e\left[n\right] = y\left[n\right] - d\left[n\right] \tag{2.30}$$

$$e\left[n\right] = y\left[n\right] - \sum_{k=0}^{M-1} w\left[k\right] s\left[n-k\right] \tag{2.31}$$

$$e\left[n\right] = y\left[n\right] - w^T\left[n\right] s\left[n\right] \tag{2.32}$$

Ahora bien, el objetivo es minimizar el error cuadrático medio:

$$\varepsilon_{MSE} = E\left\{\left|e\left[n\right]\right|^2\right\} \tag{2.33}$$

$$\varepsilon_{MSE} = E\left\{\left|e\left[n\right] e^T\left[n\right]\right|\right\} \tag{2.34}$$

$$\varepsilon_{MSE} = E\left\{\left|\left(y\left[n\right] - w^T\left[n\right] s\left[n\right]\right)\left(y\left[n\right] - w^T\left[n\right] s\left[n\right]\right)^T\right|\right\} \tag{2.35}$$

$$\varepsilon_{MSE} = Var\left\{y\left[n\right]\right\} - r_{ys}\left[n\right] w\left[n\right] - w^T\left[n\right] r_{ys}\left[n\right] + w^T\left[n\right] R_s\left[n\right] w\left[n\right] \tag{2.36}$$

Aplicando el criterio de la primera derivada respecto a $w\left[n\right]$ e igualando a 0, se obtiene lo siguiente:

$$R_s\left[n\right] w\left[n\right] = r_{ys}\left[n\right] \tag{2.37}$$

Finalmente, el estimador MMSE ($w[n]$) viene dado de la siguiente manera:

$$w\left[n\right] = R_s^{-1} r_{ys}\left[n\right] \tag{2.38}$$

2.6. OFDM (Orthogonal Frecuency Division Multiplexing)

Según [Ver08, Val10, Man08, Art07], OFDM consiste en una multiplexación en frecuencia de diferentes portadoras, donde cada una transporta una información modulada con BPSK, QPSK, 16QAM ó 64QAM. El principio básico de OFDM es dividir la secuencia de datos que debe ser transmitida a una velocidad de transmisión R símbolos por segundo, en N subcanales de datos paralelos, los cuales operan a una tasa de R/N símbolos por segundo.

Para aprovechar el ancho de banda disponible es necesaria que las subportadoras sean sobrepuestas en el espectro de frecuencia sin introducir interferencia entre subportadoras ICI (Intercarrier Interference), tal como se muestra en la Figura 2.11. Para esto, las subportadoras deben ser ortogonales entre sí, esto es:

$$\int_0^T cos\left(\omega_i t\right) cos\left(\omega_l t\right) dt = 0 \; i \neq l \tag{2.39}$$

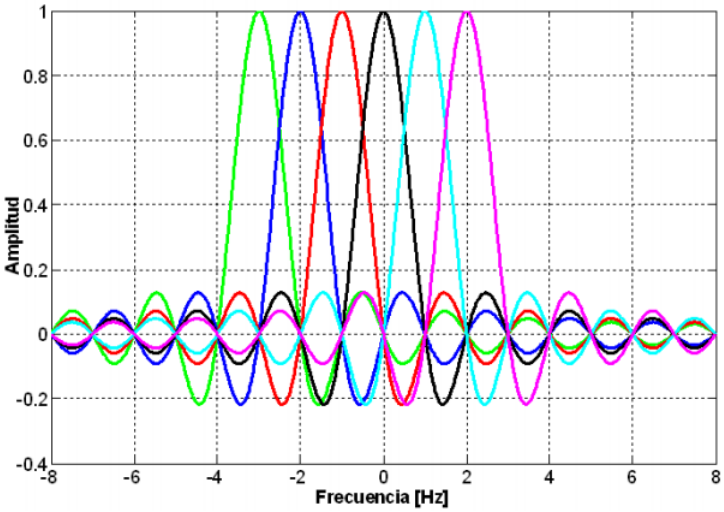

Figura 2.11.: Espectro de señal OFDM como 6 subportadoras. [LDRV07]

2.6.1. Transmisor OFDM

Para la generación de la señal OFDM es necesario utilizar un conversor serial/paralelo, de modo que la secuencia de entrada sea dividida N subcanales de datos, donde cada uno de estos subcanales contenga una subportadora compleja, formada por un seno y un coseno en la misma frecuencia [LDRV07]. Luego de ello, la sumatoria de todas las formas moduladas conforma una señal OFDM.

En el diagrama de bloques de la Figura 2.12 se observa un transmisor OFDM, el cual consta de una secuencia de datos binaria, $m(t)$, la cual es convertida por un modulador digital de fase y cuadratura en una secuencia de símbolos complejos de la forma $c_n = i_n \pm jq_n$. La componente real del símbolo, i_n, es modulada por un coseno de frecuencia ω_n, en cuanto que la componente imaginaria, q_n, es modulada por una señal sinusoidal de frecuencia ω_n.

De esta forma, el símbolo OFDM puede ser expresado:

$$s(t) = \sum_{n=0}^{N-1} i_n cos(\omega_n t) + q_n sen(\omega_n t) \tag{2.40}$$

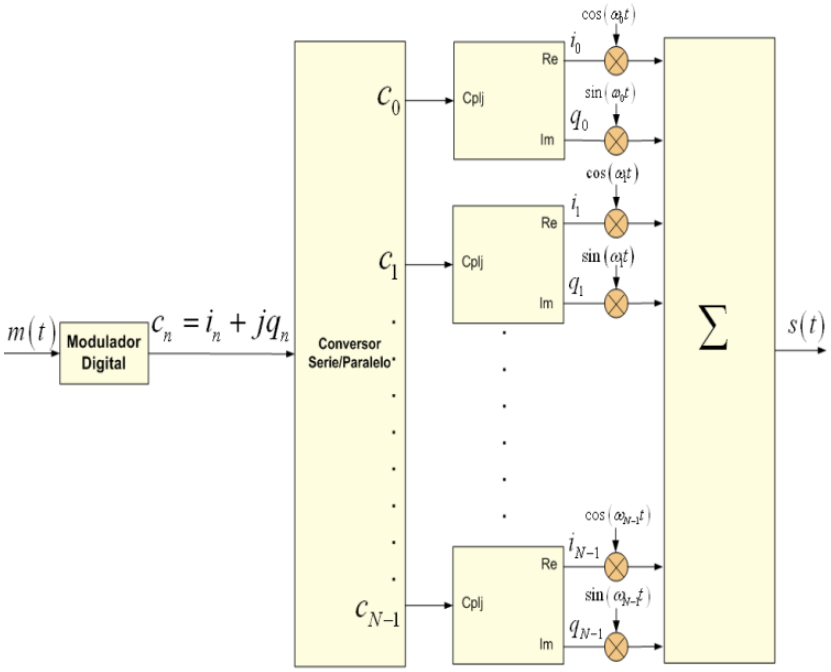

Figura 2.12.: Diagrama de Bloques de Generador de símbolo OFDM. [LDRV07]

2.6.2. Receptor OFDM

Como las funciones seno y coseno son ortogonales entre sí, entonces la señal OFDM puede ser detectada utilizando un banco de $2N$ correlacionadores, tal como se muestra en la Figura 2.13.

Es posible generar la señal OFDM a través de una serie de Fourier limitada de N elementos, donde los componentes de fase y cuadratura son los coeficientes de esta serie, por lo que la ecuación puede ser escrita:

$$s(t) = \sum_{n=0}^{N-1} Real\{i_n cos(\omega_n t) - j i_n sen(\omega_n t) + j q_n cos(\omega_n t) + q_n sen(\omega_n t)\} \tag{2.41}$$

Además, se obtiene que el espacimiento entre cada subportadora es $\frac{W}{N}$ hertz, W es el ancho de banda disponible. Por lo tanto, la frecuencia de cada subportadora viene dado por:

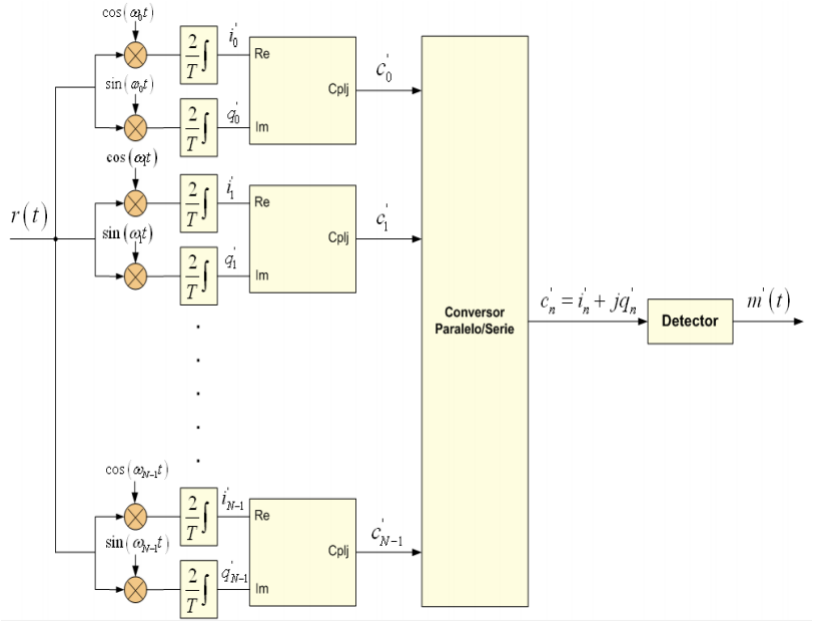

Figura 2.13.: Diagrama de Bloques Receptor OFDM con correlacionadores [LDRV07]

$$f_n = f_0 + \frac{W}{N}n \ \ , n = 0, 1, ...(N-1) \tag{2.42}$$

Debido a una relación entre la transformada de Fourier y la transformada de Fourier discreta, donde $G[n] = G\left(e^{j\omega}\right)|_{\omega_n = \frac{2\pi}{N}n}$, es posible obtener la señal OFDM discreta de la siguiente manera:

$$s[m] = \sum_{n=0}^{N-1} i_n cos\left(\frac{2\pi n}{N}m\right) + q_n sen\left(\frac{2\pi n}{N}m\right) \tag{2.43}$$

$$s[m] = Real\left\{\sum_{n=0}^{N-1} c_n e^{j\frac{2\pi n}{N}m}\right\} \tag{2.44}$$

De la ecuación anterior, la señal OFDM discreta se genera a través de las IDFT (Inverse Discrete Fourier Transform) de los símbolos c_n. Para realizar la demodulación bastaría con realizar la DFT (Discrete Fourier Transform) de la señal OFDM discreta. Pero, el tiempo de procesamiento crece de al incrementar el número de portadoras, para ello se propone la realización de la FFT (Fast Fourier Transform) que permite reducir el tiempo de generación/detección de la señal OFDM.

2.6.3. Prefijo cíclico

Los símbolos que llegan al receptor está compuesto de dos partes, una parte perteneciente a un símbolo OFDM previamente transmitido y otras pertenecientes a versiones atrasadas del propio símbolo que es denominado como ISI (Inter Symbol Interference) [LDRV07, Val10]. En la Figura 2.14 se muestra este el efecto producido por el canal.

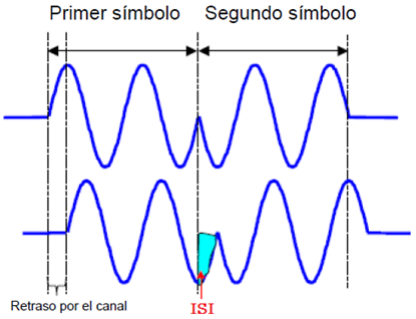

Figura 2.14.: Efecto ISI en los símbolos recibidos. [Val10]

Para minimizar este problema, se adiciona un intervalo de guarda después del símbolo resultante de la IFFT, ello garantiza la periodicidad dentro del nuevo símbolo, en la que debe cumplir $G > \tau_n$. (G: tiempo del prefijo introducido, τ_n: retardo esparcido del canal). En la Figura 2.15 se muestra el diagrama de bloques de un transmisor/receptor OFDM.

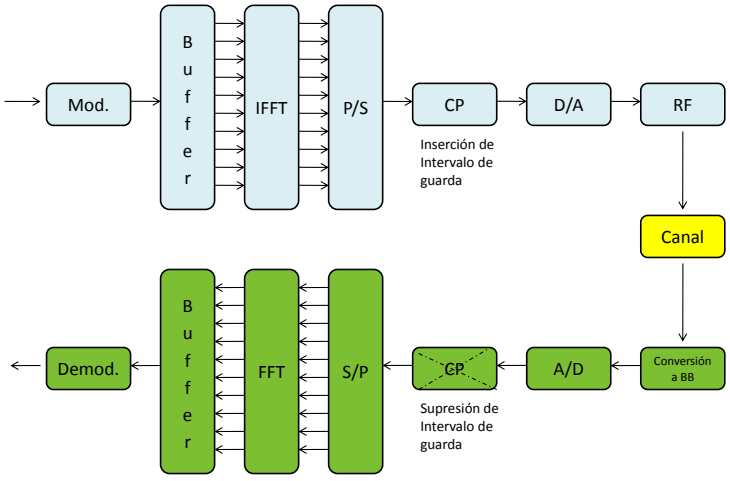

Figura 2.15.: Diagrama de Bloques de un Transmisor y Receptor OFDM. [Val10]

2.6.4. Ventajas y desventajas de OFDM

Las ventajas del uso de OFDM son:

- La eficiencia del espectro porque permite solapamiento entre subportadoras logrando transmitir altas tasas de datos en comparación con el sistema de comunicación de portadora simple.
- Reduce la ISI, gracias al uso del prefijo cíclico.
- El uso del algoritmo de la FFT permite que la generación de la señal OFDM sea más eficiente computacionalmente.

Entre las desventajas de OFDM tenemos:

- Es sensible a errores en la sincronización de la señal, por lo que ocasiona que se degrade la señal recibida al no obtenerse la ortogonalidad entre subportadoras.
- Es más complejo en comparación con el esquema de modulación de portadora simple.

3. Estado del Arte

En este capítulo se describen diferentes mecanismos propuestos que permiten incrementar el nivel de seguridad en los actuales sistemas de comunicación inalámbrica.

En [Pra10] se describe la seguridad desarrollada por el estándar IEEE 802.16 y LTE. En el estándar IEEE 802.16 se presenta las funciones de la subcapa de seguridad ubicado en la capa enlace de datos, tal como se muestra en la Fig. 3.1.

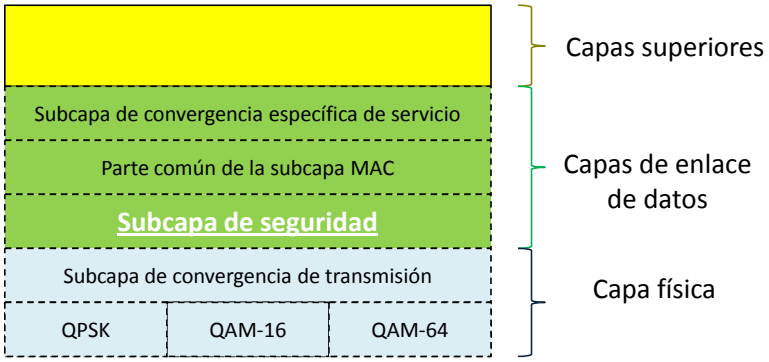

Figura 3.1.: Arquitectura de Seguridad en el Estándar IEEE 802.16. [Pra10]

En [Pra10, ZAG06] se menciona que el proceso de seguridad en el estándar IEEE 802.16 consta de tres pasos.

1. Autenticación
2. Intercambio de clave de datos.
3. Encriptación de datos, sólo los mensajes de datos son encriptados usando DES. No hay detección de la integridad del mensaje.

Los autores [CWH+11] explican algunos enfoques que permiten incrementar el nivel de seguridad a nivel de capa física. A continuación se mencionan estos enfoques así como las técnicas usadas en cada uno.

3.1. Enfoque basado en la codificación

El primer enfoque está basado en la codificación el cual ayuda a incrementar la autentificación [CWH+11]. Las técnicas que se encuentran bajo éste enfoque son el uso de códigos de corrección de errores y la codificación por espectro ensanchado.

Los autores en [VFA08] proponen una técnica que consiste de la combinación de codificación turbo y cifrado AES. Esta técnica se basa en la generación de números pseudoaleatorios que seleccciona N de M bits para luego ser codificados con turbo código. Dependiendo de la condición del canal, este método puede elegir el número de bits redundantes requeridos para proteger la información con el fin de alcanzar una alta eficiencia, logrando así que los posibles atacantes obtengan una alta tasa de error de decodificación.

Por otro lado, en [Sán00, Pov00] desarrolla la técnica de codificación por espectro ensachado, y consiste en que una señal es expandida por una secuencia pseudoaleatoria sobre una extensa banda de frecuencia. La mayor ventaja del espectro ensanchado es la alta inmunidad obtenida frente a interferencias casuales (usuarios que emplean el mismo canal) o frente a interferencias intencionales por parte de alguien que desea bloquear intencionadamente una comunicación en curso.

Según [Pov00], las ventajas más importantes de los sistemas de modulación de espectro ensanchado son:

- Baja probabilidad de ser interceptada debido al ensanchamiento del espectro.
- Alta inmunidad frente a interferencia intencionada.
- Posibilidad de acceso múltiple, con lo cual es posible tener varios usuarios cursando comunicaciones independientes en el mismo canal.

3.2. Enfoque basado en potencia

En [CWH+11] se menciona que la protección de los datos se puede realizar usando un enfoque basado en la potencia. Los esquemas tradicionales utilizan ruido. En [Goe07] se desarrolla un método que garantiza el secreto de la comunicación en un medio inalámbrico en presencia de un atacante. La idea clave consiste en degradar el canal del atacante, independientemente de su posición. El transmisor emitirá una señal con ruido artificial, de tal manera que sólo sea cancelable en el receptor, y no por un oyente no autorizado. Esta señal se puede degradar selectivamente el canal del atacante.

3.3. Enfoque basado en el Diseño de la Señal

Los autores de [GK11] desarrollan la técnica iJam que presenta dos características importantes, por un lado se encuentra la velocidad con la que se realiza y por otro lado la independencia frente a las variaciones del canal de comunicación. Esta técnica consiste en enviar muestras de la señal original y la réplica de manera aleatoria, el receptor bloquea al azar la muestra en la transmisión original, o la correspondiente muestra en la repetición tal como se muestra en la Fig. 3.2. Ahora bien, debido a que

el espía no conoce la muestra de señal que ha sido bloqueada, no podrá decodificar correctamente los datos.

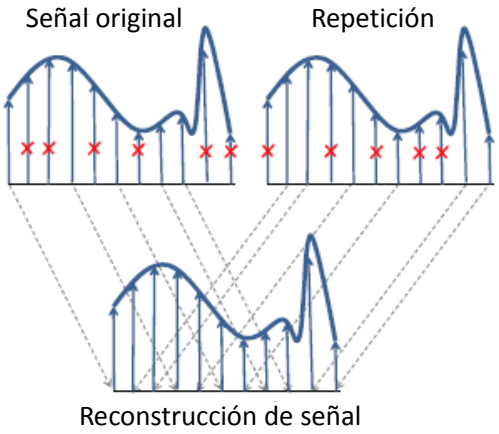

Figura 3.2.: Técnica iJam [GK11]

Los autores de [GK11] implementan esta técnica utilizando la capa física del estándar IEEE 802.11 con distintos esquemas de modulación. En esta implementación no se considera un canal con desvanecimiento multitrayecto, sino se agrega ruido AWGN sobre la señal transmitida. En la Fig. 3.3 se observa las curvas de BER obtenido para diferentes valores de SNR y esquemas de modulación.

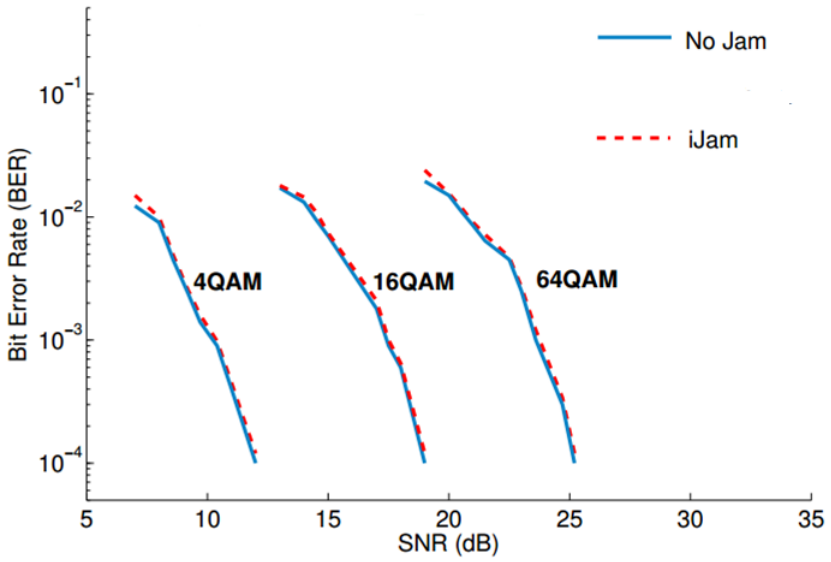

Figura 3.3.: BER obtenido con la técnica iJam [GK11]

3.4. Enfoque basado en el Canal de Comunicación

El siguiente enfoque que se describe tanto en [RL05, FS02, JST10b, JST10a, VL11], es el que usa el canal de comunicación como mecanismo de seguridad en una comunicación inalámbrica. Los autores en [JST10b, JST10a], desarrollan un esquema de seguridad el cual se muestra en la Fig. 3.4. La idea consiste en combinar dos técnicas, el cifrado para generar una clave y la pre-compensación del canal. La clave es usada para transformar la constelación de la señal original en una constelación rotada, la clave generada es conocida tanto por el transmisor como por el receptor legítimo.

Por otro lado, se asume un canal simétrico, lo que significa que el canal de comunicación es el mismo tanto para el transmisor como para el receptor, con lo que se realiza una pre-compensación del canal antes de enviar los símbolos rotados por el canal con desvanecimiento multitrayecto. Una vez realizado ello, el receptor legítimo es capaz de decodificar los símbolos enviados a través de la rotación de los símbolos utilizando la misma clave generada.

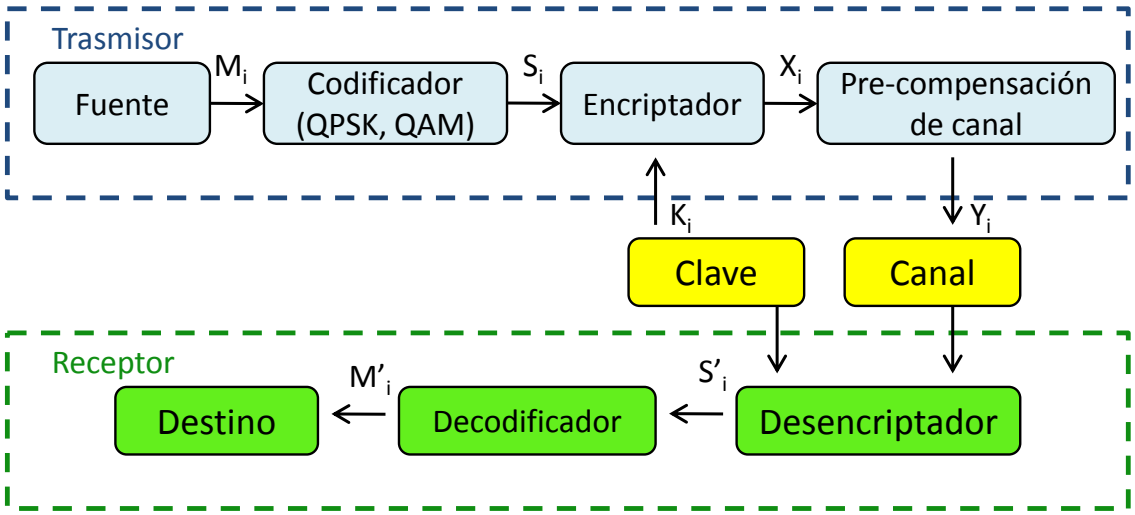

Figura 3.4.: Sistema de Seguridad usando Rotación de Símbolos [JST10a]

Así mismo, los autores [JST10b, JST10a] implementan esta técnica utilizando una modulación QPSK sobre un canal multitrayecto al que se le agrega ruido AWGN.

La medida de seguridad se basa en el BER, y el objetivo es que el atacante presente una curva de BER casi constante conforme los valores de Eb/No se incrementen, al mismo tiempo en el receptor legítimo presente una curva de BER decreciente bajo las mismas condiciones. En la Fig. 3.5 se compara las curvas de BER para el receptor legitimo, el espía y la curva teórica.

Los autores en [YWG+15] explican que la seguridad en capa física es un tema clave que debe ser implementado en el nuevo estándar 5G, esto dado que los sistemas

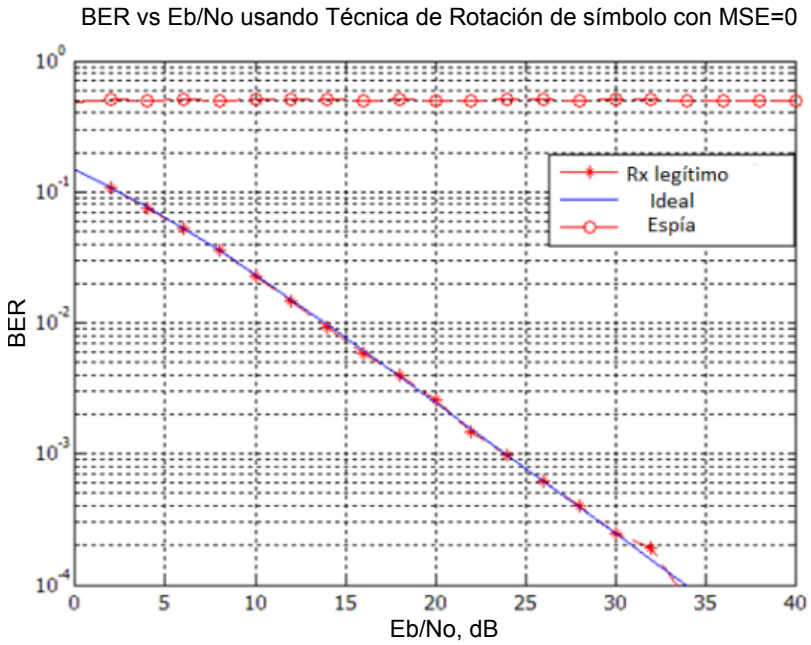

Figura 3.5.: BER obtenido con el Sistema de Seguridad usando rotación de Símbolos [JST10a]

tradicionales no serán una solución definitiva para asegurar la seguridad de la información que se transmite a través de las interfaces inalámbricas. Una de las ventajas del uso de las técnicas de seguridad en capa física es que no dependen de la capacidad computacional de un posible atacante, además las técnicas de seguridad en capa fisica presentan una alta escalabilidad.

3.5. Resumen

Los autores [Pra10, ZAG06] explican la seguridad que se implementa en los estándares IEEE 802.16 y LTE y esta se basa en la autenticación de los nodos antes de que acceda a la red, este proceso de auntenticación se da en la capa de enlace de datos. Por otro lado, los autores [CWH+11] explican algunos enfoques que se han venido desarrollando para incrementar el nivel de seguridad en redes inalámbricas a nivel de capa física. El enfoque basado en la codificación con espectro ensanchado es usado en los actuales sistemas de comunicación celular como CDMA, WCDMA, sin embargo, presenta algunos inconvenientes como es el incremento de ruido al tener a todos los nodos transmitiendo en la misma banda de frecuencias. El enfoque basado en el diseño de señal presenta la ventaja que no es afectado por el canal; sin embargo, requiere transmitir la misma señal dos veces provocando una ineficiencia en cuanto al uso de ancho de banda y energía. La técnica basado en el canal de comunicación presenta la ventaja que este no es el mismo para ninguno de los nodos y se puede

diferenciar, sin embargo en la técnica mencionada se requiere una sincronización perfecta entre transmisor/receptor para que la rotación generada por la clave sea conocida en ambos extremos. Finalmente, se estima que en el nuevo estándar 5G se implemente tecnicas de seguridad en capa fisica dado que los sistemas criptográficos tradicionales no serán capaces de asegurar la información que se transmite a través de las interfaces inalánbricas.

4. Propuesta de Solución

En este capítulo se presenta la solución al problema expuesto. En la Sección 4.1 se presenta el escenario del problema a resolver, considerando al transmisor y receptor legítimo en presencia de un atacante. El detalle de cada uno de los procesos y el desarrollo matemático de la solución propuesta son descritos en la Sección 4.2

4.1. Escenario de la Solución Propuesta

El escenario donde se desarrolla la propuesta es mostrado en la Figura 4.1. Se considera los siguientes puntos:

- Existen dos nodos de comunicación, transmisor y receptor legítimo.
- Los nodos utilizan antenas omnidireccionales.
- Se tiene la presencia de un atacante.
- La potencia de transmisión del Nodo A y del Nodo B son iguales.

La presente propuesta, analiza el peor caso que se puede presentar en una comunicación inalámbrica, esto es, cuando el espía está incluido dentro del rango de cobertura del transmisor y del receptor, ya que éste puede escuchar tanto la transmisión del nodo A como la del nodo B.

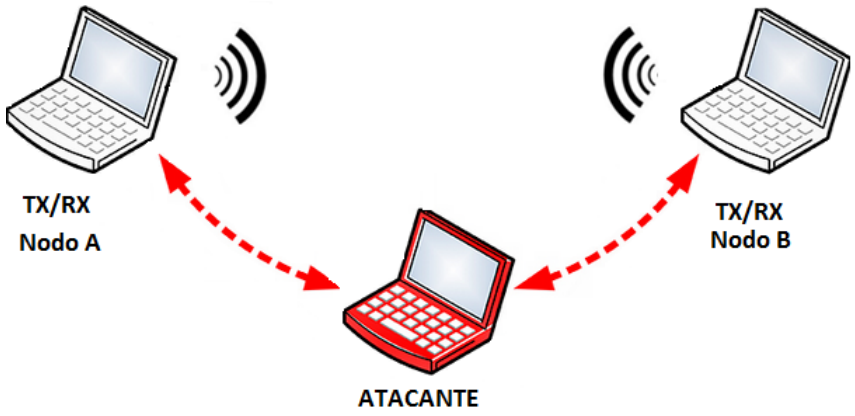

Figura 4.1.: Escenario del Problema Estudiado

4.2. Descripción de la Solución Propuesta

Para establecer una comunicación entre los nodos A y B, es necesario realizar un intercambio inicial de símbolos, denominado proceso de saludo. El objetivo de este proceso es establecer un acuerdo previo entre los nodos de comunicaciones para poder enviar información. Además, se puede estimar el canal en el receptor legítimo y realizar la descomposición matricial del canal de modo que una de las matrices sea enviada hacia el transmisor, quien se encargará de transmitir los símbolos codificados. En la siguiente sub-sección se describe el proceso de saludo.

4.2.1. Proceso de Saludo

En primer lugar existirá un intercambio de símbolos entre los nodos A y B antes de enviar la información propiamente dicha. Este proceso se realiza con el fin de poder estimar el canal en el receptor legítimo y realizar la descomposición matricial del canal de modo que una de las matrices sea enviada hacia el transmisor, quien se encargará de transmitir los símbolos codificados. Este proceso se muestra en la Figura 4.2.

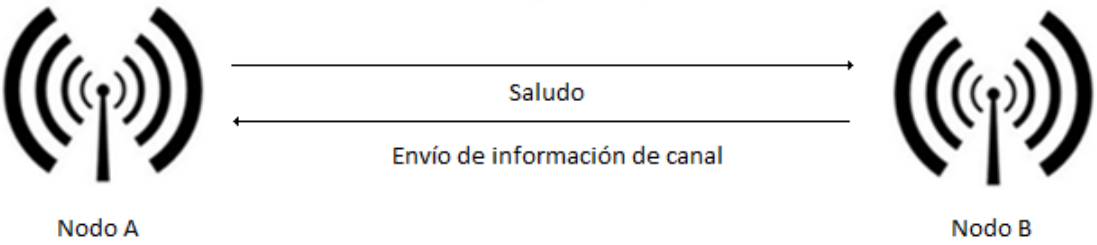

Figura 4.2.: Proceso de Saludo

El detalle de cada trama se describe a continuación.

Primera trama: Considerada como una trama de saludo enviada por el Nodo A hacia el Nodo B, contiene un patrón de bits (secuencia fija).

Segunda trama: El Nodo B recibe el patrón de bits y con ellos estima el canal, una vez realizado ello, procede a la descomposición matricial de donde se obtienen tres matrices U_k, Δ_k y V_k. La matriz V_k es enviada al transmisor, quien se encargará de codificar los datos.

4.2.2. Desarrollo de la Solución Propuesta

En esta sección se desarrolla la parte de la solución propuesta. A continuación se consideran algunos supuestos que se han tomado en cuenta.

Supuestos:

- Se supone que se ha desarrollado previamente el proceso de autenticación entre el transmisor y el receptor, este proceso implica la identificación de usuarios legítimos, llevándose a cabo antes del proceso de encriptación de datos. Se debe tener en consideración que los problemas referidos a autenticación y husmeo son independientes y la presente propuesta es aplicable para los ataques de husmeo.
- Se supone que el proceso de saludo es realizado con éxito entre los nodos de comunicación.
- Se supone que existe el hardware adecuado para poder desarrollar el mecanismo propuesto.
- Se considera que el atacante cuenta con un canal de propagación H_{ka} distinto al del receptor legítimo H_k. Esto debido a que se considera que el atacante se encuentra a una distancia mayor a media longitud de onda (aprox. mayor a 6cm. en sistemas OFDM convencionales), con lo que el canal de propagación es variante en tiempo y espacio.
- El tipo de canal de propagación es modelado con un filtro FIR en la que la respuesta al impulso sigue la distribución de Rayleigh.
- El tipo de ruido que se añade es AWGN (Additive White Gaussian Noise).

La solución propuesta se desarrolla en la capa física, específicamente en el bloque del canal de propagación. Se propone realizar un cambio en los símbolos de transmisión OFDM, los que serán multiplicados con la matriz V_k, obtenida al realizar la descomposición SVD a la matriz de propagación H_k. El diagrama de bloques del sistema de seguridad propuesto se muestra en la Figura 4.3.

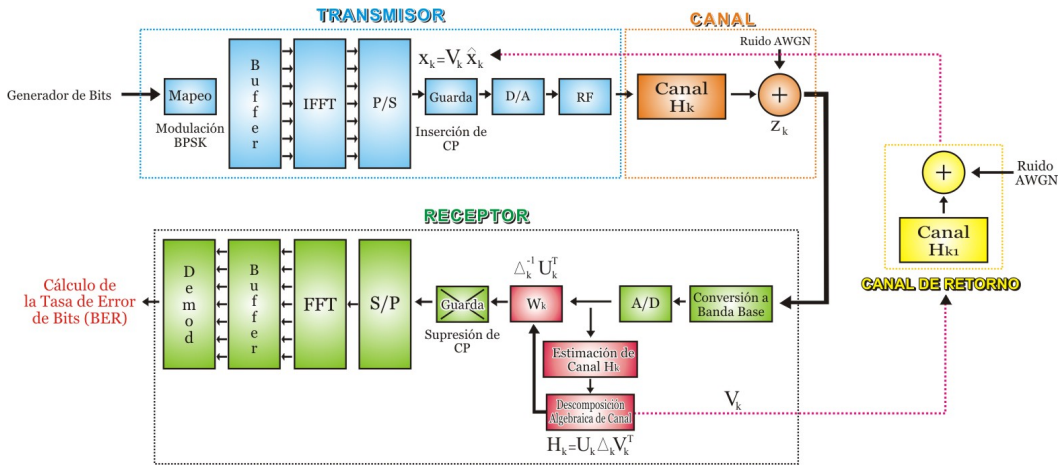

Figura 4.3.: Diagrama de Bloques del Sistema de Seguridad.

4.2.2.1. Descomposición Algebraica del Canal de Propagación

Durante el proceso de saludo se asume que el transmisor envía una cierta cantidad de símbolos al receptor legítimo. Estos símbolos servirán para que el receptor pueda estimar el canal, una vez realizado ello, el receptor realizará la descomposición algebraica del canal estimado, donde se obtiene tres matrices, una de las matrices V_k es transmitida del receptor al transmisor, para que con ella comience el proceso de encriptación de la información. Así mismo el receptor debe tener una matriz desencriptadora W_k esta matriz consta de la matriz unitaria U_k y la matriz diagonal Δ_k.

$$W_k = \Delta_k^{-1}.U_k^T \tag{4.1}$$

A continuación se detalla paso a paso el proceso de encriptación y desencriptación de datos.

Sea h el canal de propagación modelado entre el transmisor y receptor legítimo, el cual puede ser descrito como un filtro FIR de L coeficientes complejos de la forma:

$$h = [h\,(0)\ h\,(1) \ldots h\,(L-1)] \tag{4.2}$$

Ahora bien, podemos definir la matriz de convolución de canal H_k como una matriz cuadrada Toeplitz de tamaño $k\,x\,k$, donde la primera columna de la matriz esta dado por $\left(h^T,\, \theta_N^T\right)$ y la primera fila viene dado como $(h\,(0)\,,\, \theta_{k-1})$, donde $N = k - L + 1$ y $\theta_M$es un vector fila de $M - ceros$, por lo que la matriz H_k puede ser definida como:

$$H_k = \begin{bmatrix} h\,(0) & 0 & 0 & \cdots & 0 & 0 \\ h\,(1) & h\,(0) & 0 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ldots & \vdots & \vdots \\ h\,(L-1) & h\,(L-2) & h\,(L-3) & \cdots & h\,(0) & 0 \\ 0 & h\,(L-1) & h\,(L-2) & \cdots & h\,(1) & h\,(0) \end{bmatrix} \tag{4.3}$$

Mediante el uso de la descomposición en valores singulares, descomponemos la matriz H_k en tres matrices representadas de la siguiente forma:

$$H_k = U_k \Delta_k V_k^T \tag{4.4}$$

Donde U_k y V_k son matrices cuadradas de dimensiones $k \times k$ que contienen los vectores singulares izquierdo y derecho del canal H_k respectivamente. La matriz diagonal cuadrada Δ_k de dimensiones $k \times k$ contiene los valores singulares o eigenvalores. Cada símbolo generado por medio de la modulación OFDM es representado como un vector de k-elementos de la siguiente forma:

$$\hat{x_k} = \left[\hat{x^1}\hat{x^2}\dots\hat{x^k}\right]^T \tag{4.5}$$

A continuación se utiliza la matriz V_k como matriz encriptadora, la cual multiplica a cada símbolo transmitido, con lo que cada símbolo transmitido es:

$$x_k = V_k\hat{x_k} \tag{4.6}$$

Por lo tanto, los símbolos recibidos al pasar por el canal matricial H_k y al ser sumados por una componente de Ruido AWGN, z_k, serán representados de la siguiente forma:

$$y_k = H_k V_k \hat{x_k} + z_k \tag{4.7}$$

Una vez recibido cada símbolo, se procede a realizar el proceso de desencriptación, ello se logra multiplicando el símbolo recibido por la matriz W_k. Finalmente, cada símbolo desencriptado en el receptor tiene la forma de:

$$\hat{x^{,}} = \hat{x_k} + z_k^{,} \tag{4.8}$$

Donde la componente de ruido $z_k^{'}$ viene dado por:

$$z_k^{'} = \Delta_k^{-1} U_k z_k \tag{4.9}$$

En la Figura 4.4 se muestra el Diagrama de bloques del proceso descrito anteriormente:

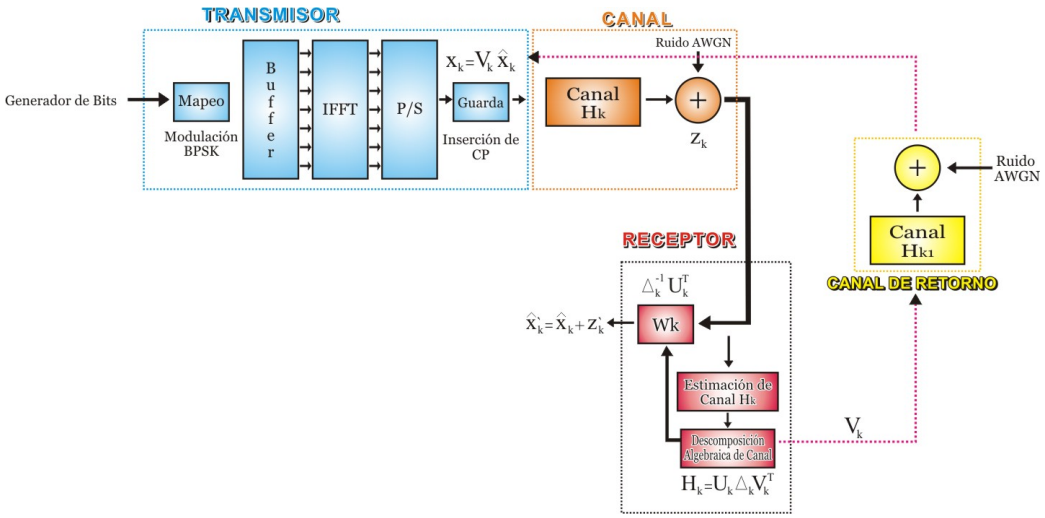

Figura 4.4.: Diagrama de Bloques del Transmisor/Receptor OFDM usando SVD.

La demostración matemática de este proceso es desarrollado de manera detallada en el Apéndice A.

5. Simulaciones y resultados

5.1. Software

Las simulaciones realizadas en este capítulo fueron hechas con el software MATLAB R2009a. MATLAB es un entorno de programación para el desarrollo de algoritmos, análisis de datos, visualización y cálculo numérico [Mat].

5.2. Simulación de los Estimadores de Canal

En esta sección se realiza la simulación de los estimadores de canal, esto nos permitirá elegir el algoritmo de estimación de canal a utilizar en el presente trabajo. La simulación se basa en la especificación IEEE 802.11a. en banda base. El detalle se describe a continuación.

- Se generan 10000 símbolos OFDM, cada símbolo consta de 64 subportadoras, de las cuales 52 subportadoras incluyen información de datos y pilotos, mientras que 12 subportadoras son nulas, tal como se muestra en la Figura 5.1.
- A la entrada se tiene una trama serial de 52 bits aleatorios con distribución uniforme.
- Estos bits pasan a un formato paralelo y son modulados con BPSK, además se inserta 12 bits nulos, estos bits se encuentran en la posición 1 y desde la posición 28 hasta la 38, generando así una trama de 64 bits.
- A cada uno de los bits se le asigna una subportadora a través de la IFFT y se efectúa la normalización de la señal generada.
- Se realiza la conversión paralela a serie a la salida de la IFFT y se le agrega el prefijo cíclico para combatir los efectos del canal multitrayectoria.
- La transmisión de los símbolos se realizan sobre un canal normalizado que agrega desvanecimiento multitrayecto, éste canal es modelado como un filtro FIR de 10 etapas, en la que la respuesta al impulso sigue la distribución de Rayleigh, además se le añade ruido gaussiano normalizado de media cero y varianza unidad.
- Dado que la energia de la señal es fijada, para obtener la variación del error se ha ido disminuyendo la energía de ruido para obtener valores desde $SNR = 0$ hasta $SNR = 25$.

- En el receptor se elimina el prefijo cíclico.
- Se realiza la estimación de canal con los algoritmos LSE y MMSE y se compara el error cuadrático medio obtenido para diferentes valores de SNR.

De acuerdo a [Mat13], los valores de SNR que se realiza en la simulación pueden ser calculados de la sgte. manera:

$$SNR_{dB} = \left(\frac{N}{N_{cp}+N}\right)_{dB} + \left(\frac{N_{st}}{N}\right)_{dB} + \left(\frac{E_b}{N_o}\right)_{dB} \tag{5.1}$$

donde:

N_{st} : Número de subportadoras de datos, N : Tamaño de la FFT , N_{cp} : Número de subportadoras añadidas por el prefijo cíclico.

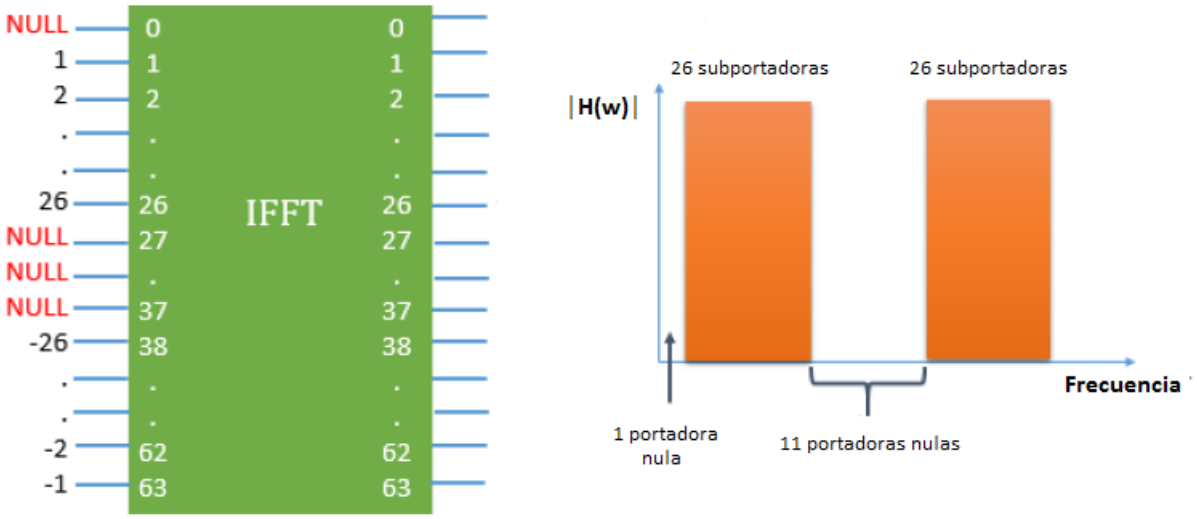

Figura 5.1.: Asignación de subportadoras en la especificación IEEE 802.11.

En la Figura 5.2 se aprecia el diagrama de bloques que se ha realizado para el desarrollo de esta simulación.

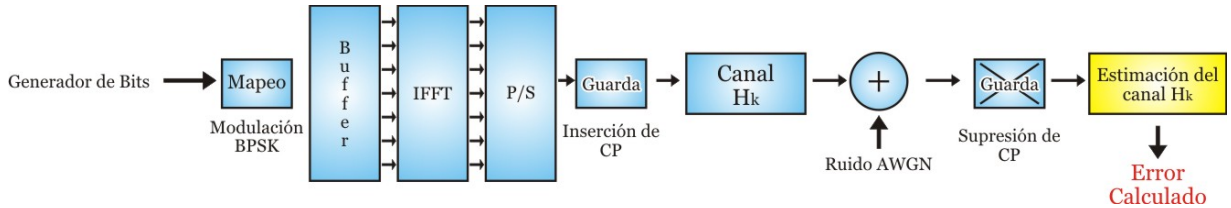

Figura 5.2.: Diagrama de Bloques para el cálculo del error usando LSE y MMSE.

En el Cuadro 5.1 se muestra los parámetros de simulación.

Parámetro	Valor
Número de subportadoras de datos:	52
Número de IFFT/FFT	64
Separación entre subportadoras	$0.3125Mhz$
Duración de Prefijo Cíclico	$0.8us$
Período de símbolo	$4us$
Retardo esparcido del canal	$0.5us$
Ancho de banda	$20Mhz$
Número de símbolos	10000
Duración de la muestra	$4\ ms$
Periodo de muestreo	$0.0125\ us$

Cuadro 5.1.: Parámetros de Simulación basado en el estándar IEEE 802.11a.

En la Figura 5.3 se muestra las curvas del MSE (Minimun Square Error) obtenidos con los algoritmos LSE y MMSE. Se puede apreciar que el estimador MMSE tiene un menor error en comparación del LSE, esto se produce porque en la derivación de MMSE se ha supuesto el conocimiento de la correlación del canal y la varianza de ruido.

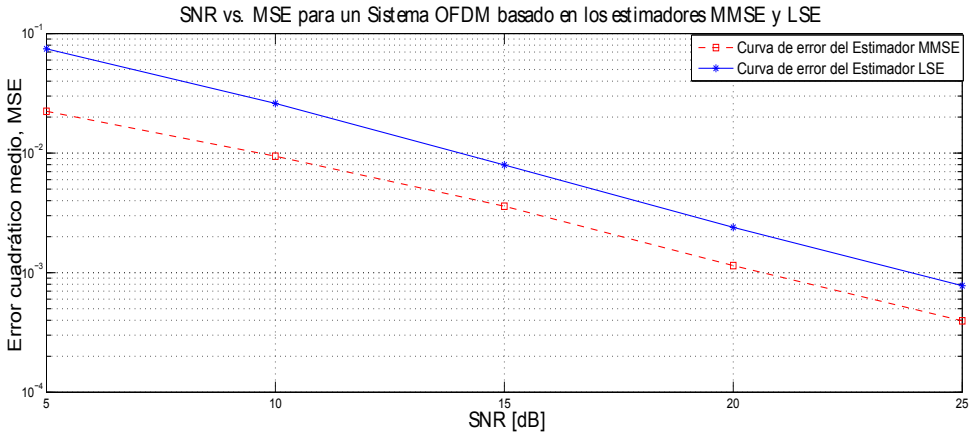

Figura 5.3.: Error de Estimación para LSE y MMSE.

El modelo de estimación de canal MMSE emplea un mayor número de recursos de procesador, lo cual se traduce en mayor tiempo de ejecución, esto debido a que se introduce un mayor número de cálculos y mayor complejidad que los requeridos por el algoritmo LSE. Pero a pesar de emplear mayores recursos, es conveniente su utilización frente al algoritmo LSE, ya que la diferencia en cuanto al error producido entre ambos modelos es bastante grande. Además, el uso del estimador MMSE es

conveniente para el caso que presentamos ya que es importante conocer el canal de una manera óptima en el transmisor, porque es el canal quien nos proporciona la seguridad frente a los atacantes.

5.3. Simulación del Sistema de Seguridad en Capa Física

En esta sección se implementa la simulación de la Capa Física basado en el Estándar IEEE 802.11a en banda base, se detalla la función el comportamiento que experimenta la señal sobre de cada uno de los bloques. En la Figura 5.4 se muestra el diagrama de bloques del sistema de comunicación que se ha simulado. Los parámetros de simulación son de acuerdo a lo presentado en el Cuadro 5.1.

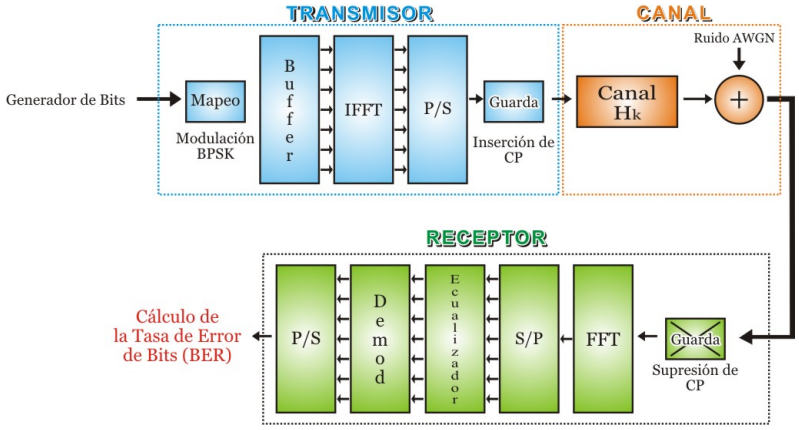

Figura 5.4.: Diagrama de Bloques de la Capa Física según el estándar IEEE 802.11a.

5.3.1. Transmisor

El transmisor genera una secuencia de 0's y 1's con distribución uniforme. La secuencia generada ingresa al conversor serial/paralelo quien se encarga de realizar el formateo de los datos a las dimensiones adecuadas para la transmisión. El modulador BPSK mapea los datos, dándole un valor de fase a cada uno de los bits de entrada. Luego, se utiliza la IFFT para asignar una subportadora a cada bit generándose el símbolo OFDM. Según el estándar 802.11a, cada símbolo consta de 52 subportadoras de datos y 12 subportadoras nulas.

A continuación se inserta el CP (prefijo cíclico),en nuestro caso se ha añadido un prefijo cíclico que tiene una duración de 0.8 μs. En la Figura 5.5 se muestra un símbolo enviado (Figura 5.5a) y su densidad espectral de potencia asociada al símbolo antes de añadir el prefijo cíclico (Figura 5.5c) y después de añadir el prefijo cíclico (Figura 5.5d)

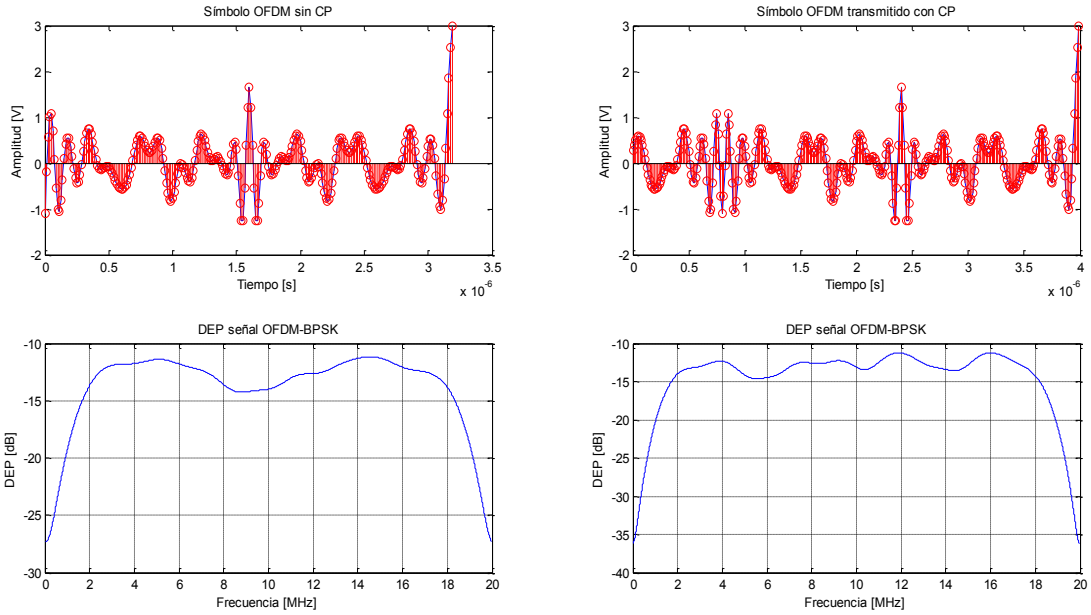

Figura 5.5.: a) Símbolo OFDM. b) Símbolo OFDM con CP. c) Densidad espectral del símbolo OFDM sin CP. d) Densidad espectral del símbolo OFDM con CP.

5.3.2. Canal

El canal de comunicación está modelado como un filtro FIR de 10 etapas con respuesta al impulso que sigue el modelo de Rayleigh, y al que se le agrega ruido gaussiano normalizado de media cero y varianza unidad.

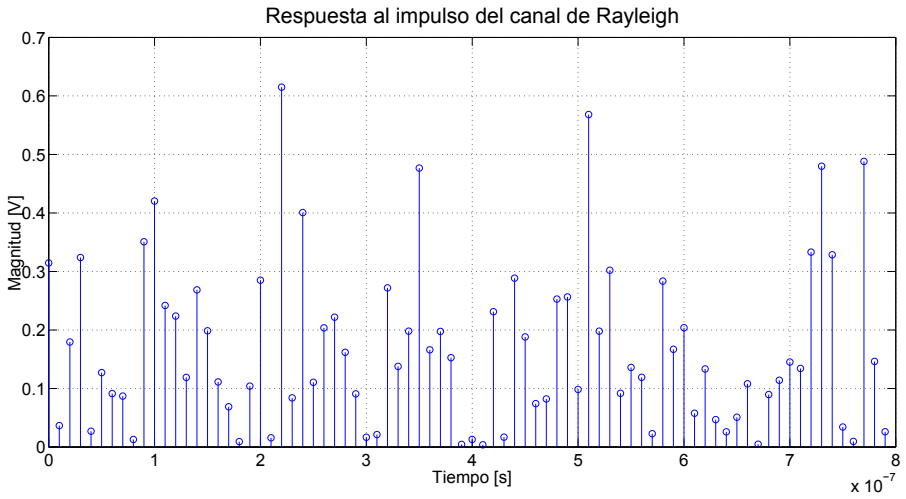

Figura 5.6.: Respuesta al impulso del canal modelado.

En la Figura 5.6 se aprecia la respuesta al impulso del canal generado. Notemos que el retardo esparcido τ_n < período de símbolo ($0.8us < 4us$). En la Figura 5.7 se muestra la función de densidad de probabilidad obtenida del canal modelado.

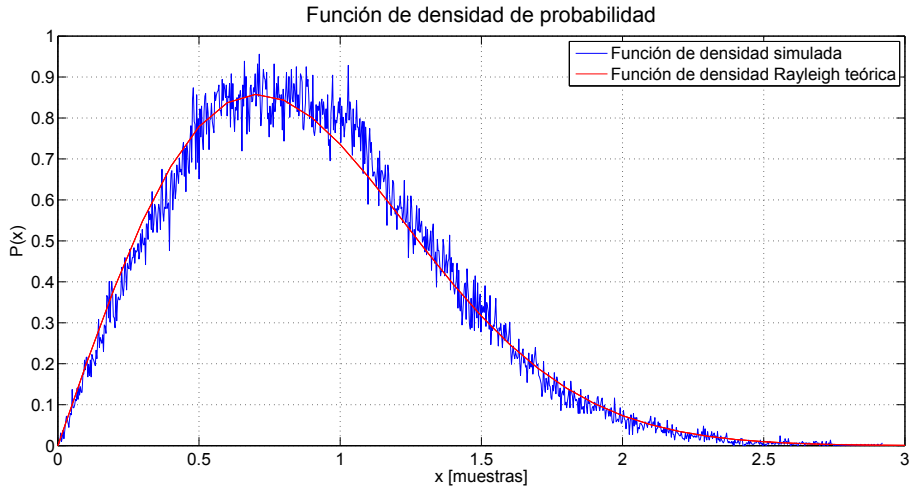

Figura 5.7.: Función de densidad de probabilidad del canal.

5.3.3. Receptor

En el receptor se elimina el prefijo cíclico, cada subportadora es demodulada utilizando la FFT, luego se realiza la conversión serial/paralelo. El bloque que se añade es el ecualizador, esto se realiza con el fin de compensar la distorsión producida por la propagación multicamino. La señal que llega al receptor viene dada por:

$$Y_m = H\left(f_m\right).X_m + Z_m \tag{5.2}$$

Si utilizamos un ecualizador con el fin de compensar la distorsión, entonces la señal ecualizada será:

$$Y_m^{'} = \frac{Y_m}{\hat{H}\left(f_m\right)} = \frac{H\left(f_m\right)}{\hat{H}\left(f_m\right)}.X_m + \frac{Z_m}{\hat{H}\left(f_m\right)} \tag{5.3}$$

En el escenario de simulación realizado se ha supuesto un conocimiento de canal ($H\left(f_m\right) = \hat{H}\left(f_m\right)$).

La Tasa de Error de Bit, que consiste en obtener la distancia euclidea entre los bits demodulados y los bits transmitidos, viene dado por:

$$BER = \frac{1}{2}\left(1 - \sqrt{\frac{\frac{E_b}{N_o}}{\frac{E_b}{N_o} + 1}}\right) \tag{5.4}$$

5.3.4. Simulación de la Capa Física basada en el Estándar IEEE 802.11a usando seguridad

En la Figura 5.8 se muestra el diagrama de bloques que se usa en la simulación. Los bloques que se han agregado son: Estimación de canal y la descomposición algebraica del canal estimado. Una de ellas, la matriz V_k, se utiliza para encriptar la información que se envía, ya que esta multiplica al vector de símbolos a enviar. Por otro lado en el receptor se tiene una matriz de desencriptación W_k, esta matriz se ha obtenido luego de realizar la SVD sobre el canal estimado, W_k multiplica a la señal recibida y_k, lo que resulta en una señal desencriptada afectada por una componente de ruido z_k.

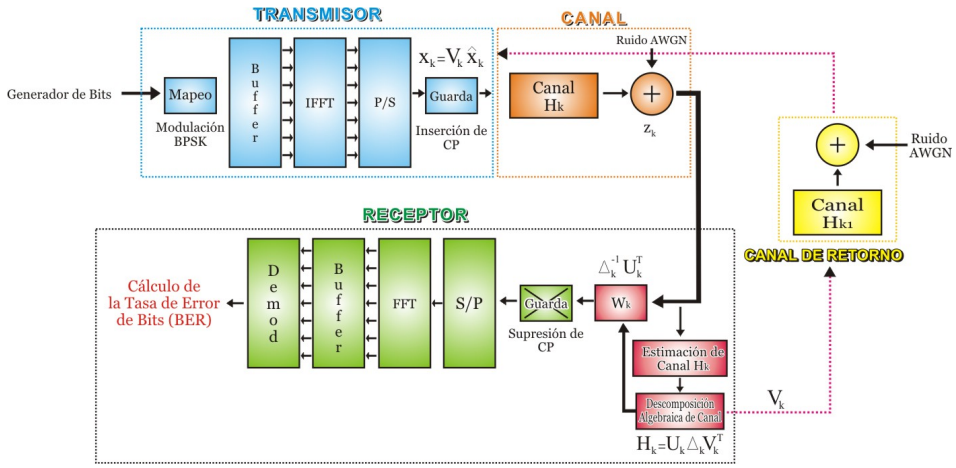

Figura 5.8.: Diagrama de Bloques del Sistema de Seguridad en Capa Física.

El primer escenario de simulación se presenta en la Figura 5.9, el atacante realiza la Descomposición Algebraica de su canal estimado H_{ka}, de modo que intenta desencriptar los datos que han sido multiplicados con la matriz V_k . La estimación de canal que realiza cada uno es distinta($H_k \neq H_{ka}$).

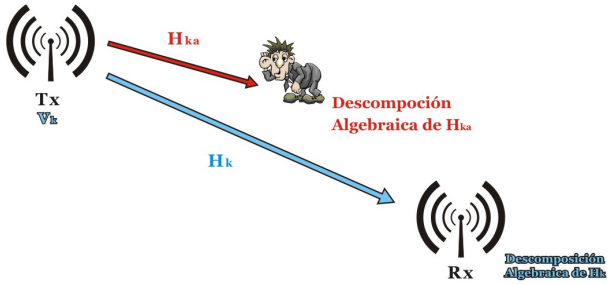

Figura 5.9.: Escenario de simulación donde el atacante realiza SVD de su canal.

En la Figura 5.10 se aprecia una variación en la densidad espectral del símbolo encriptado en comparación del símbolo sin encriptar, la matriz V_k provoca una atenuación en toda la banda de frecuencia.

A continuación, en la Figura 5.11 se muestran la respuestas al impulso de los canales del receptor legitimo y del espía.

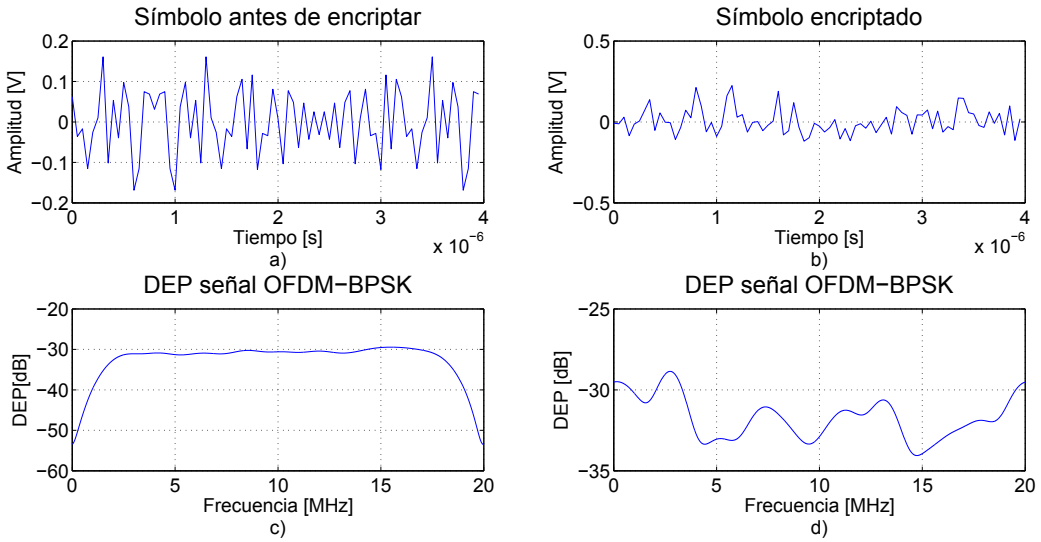

Figura 5.10.: a) Símbolo sin encriptación. b) Símbolo encriptado. c) Densidad espectral de potencia del símbolo sin encriptación. d) Densidad espectral de potencia del símbolo encriptado.

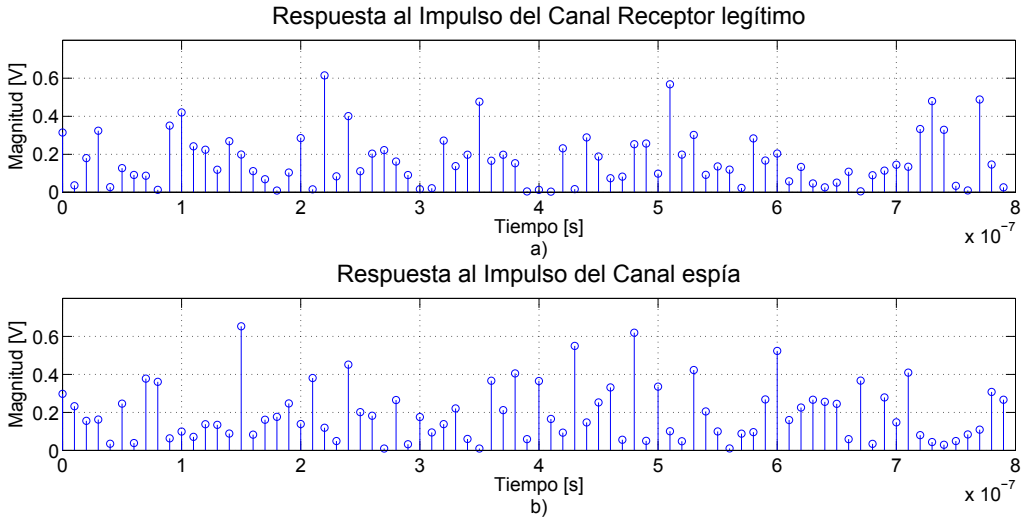

Figura 5.11.: a) Repuesta al impulso del canal del receptor legítimo. b) Respuesta al impulso del canal espía.

En la Figura 5.12 se muestra el ruido AWGN generado. Del mismo modo, se muestra la señal de ruido que es multiplicada por la matriz W_k ello con el fin de conocer cómo este factor afecta a la señal de ruido en el receptor.

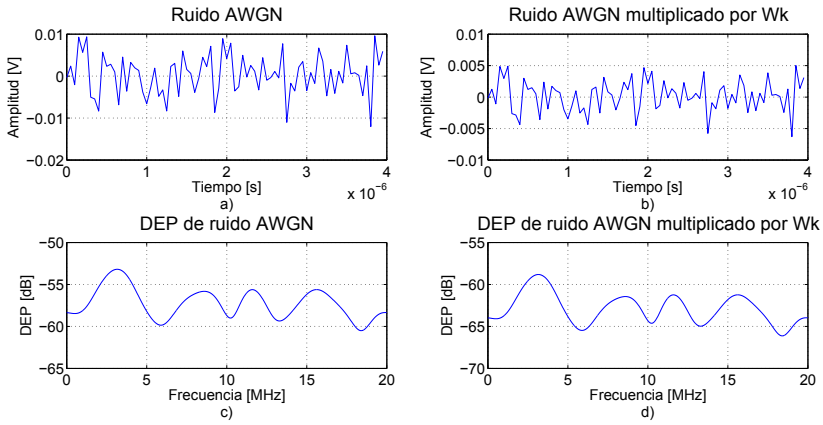

Figura 5.12.: a) Ruido AWGN. b) Ruido AWGN multiplicado por W_k. c) Densidad espectral del ruido AWGN. d) Densidad espectral del ruido AWGN multiplicado W_k.

En la Figura 5.13 se presenta la función de densidad de probabilidad obtenida por la componente de ruido $z_k^{'} = W_k z_k$. se demuestra que se mantiene el carácter de gaussiano blanco.

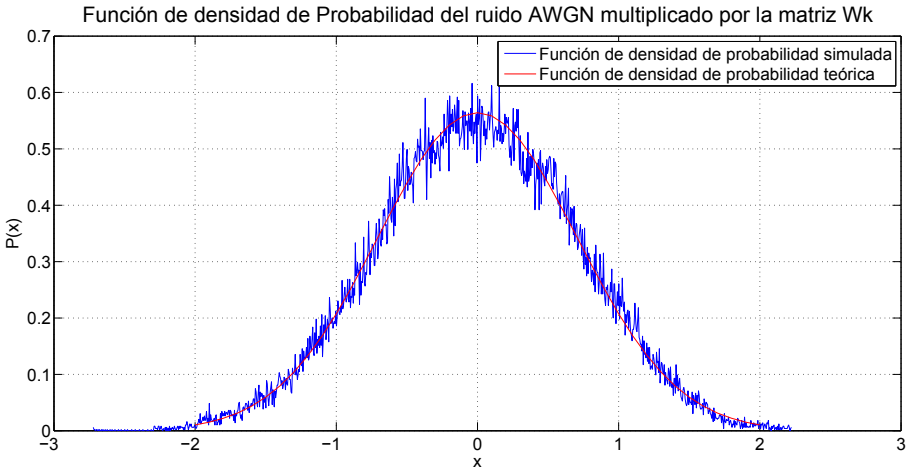

Figura 5.13.: Función de densidad de probabilidad obtenida del producto entre el ruido AWGN y la matriz W_k.

En la Figura 5.14 se compara el símbolo enviado sin encriptación (Figura 5.14a) y el símbolo recibido desencriptado(Figura 5.14b).

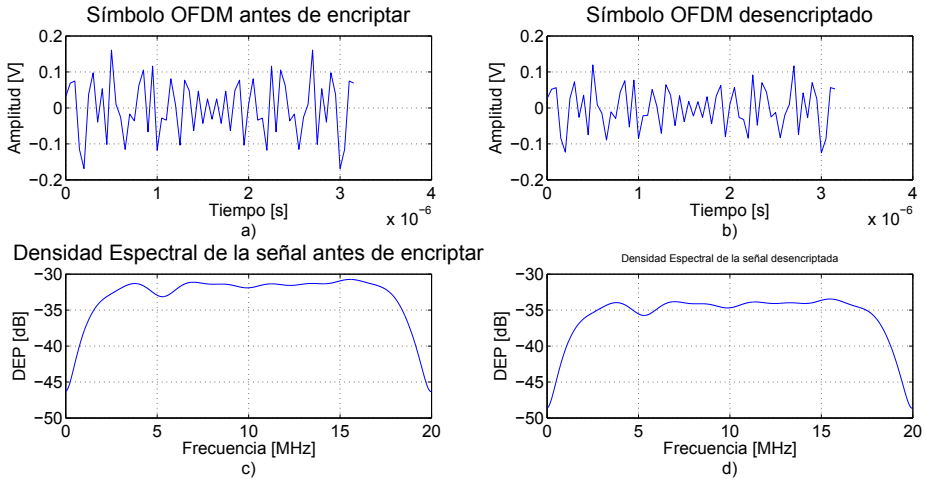

Figura 5.14.: a) Símbolo transmitido sin encriptación. b) Símbolo recibido desencriptado. c) Densidad espectral del símbolo transmitido sin encriptación. d) Densidad espectral del símbolo desencriptado.

En la Figura 5.15 se compara las curvas de BER del receptor en los sgtes estados: a)SVD con MSE=0, b)utilizando la técnica SVD con estimación de canal, c) utilizando la rotación de símbolos y MSE =0 y d) Sin conocimiento del canal (canal del atacante).

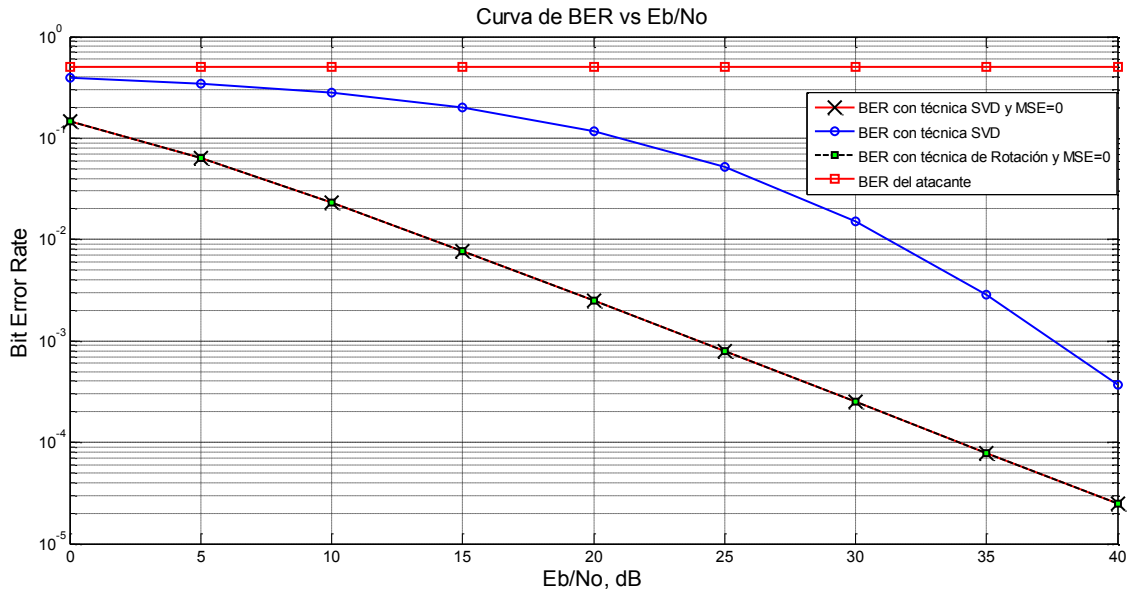

Figura 5.15.: Curva de BER vs E_b/N_o.

Como se puede apreciar, existe una diferencia entre las curvas del receptor legítimo y del atacante. Para el atacante, la cantidad de errores cometidos es considerable, llegando a ser constante para los diferentes valores de E_b/N_o. En tanto, la curva de BER del receptor legítimo cae conforme los valores de E_b/N_o se incrementan.

Asi mismo, se realiza la comparación con la técnica descrita por los autores [JST10b, JST10a]. Se aprecia que ambas técnicas presentan curvas de BER para el atacante casi constante para diferentes valores de E_b/N_o. En tanto para el caso del receptor legitimo el mecanismo propuesto por los autores [JST10b, JST10a] presenta una ganancia de codificación de 10 dB aprox., esto debido principalmente a dos aspectos, el primero es que en la técnica de rotación de símbolo el transmisor tiene conocimiento perfecto del canal de comunicación (MSE=0) con lo cual envía la información precompensando el canal que es perfectamente conocido, y segundo que se asume un perfecto sincronismo para que tanto el transmisor como el receptor conozcan la clave generada de rotación de símbolos. En la misma Figura 5.15 se hace una comparación entre ambas técnicas bajo el escenario de conocimiento perfecto de canal y se observa que la curva es la misma, esto dado que no se tiene afectación del canal de Rayleigh.

A continuación, se presenta un segundo escenario de simulación, el cual se muestra en la Figura 5.16, donde ahora el atacante no realiza la descomposición algebraica de su canal estimado H_{ka}, y él asume que la información no está siendo encriptada.

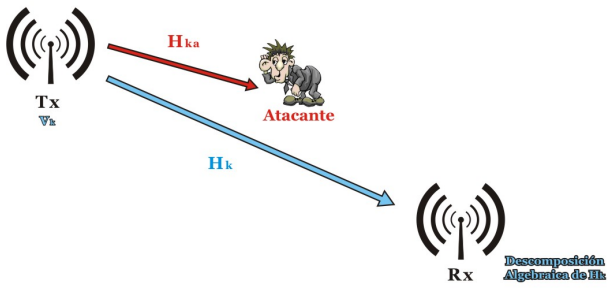

Figura 5.16.: Escenario de simulación donde el atacante no realiza SVD de su canal.

El procedimiento para realizar este escenario de simulación es el mismo que el ya expuesto anteriormente, el objetivo es revisar el comportamiento de la curva de BER del atacante. La Figura 5.17 muestra las curvas de BER del atacante cuando conoce que se ha realizado la encriptación de datos e intenta realizar su propia descomposición algebraica de Canal y cuando el atacante desconoce que los símbolos transmitidos presenten algún tipo de encriptación. Ambas curvas muestran que el BER es casi constante para diferentes valores de E_b/N_o con valores que oscilan entre $10^{-0,3}$ y $10^{-0,31}$.

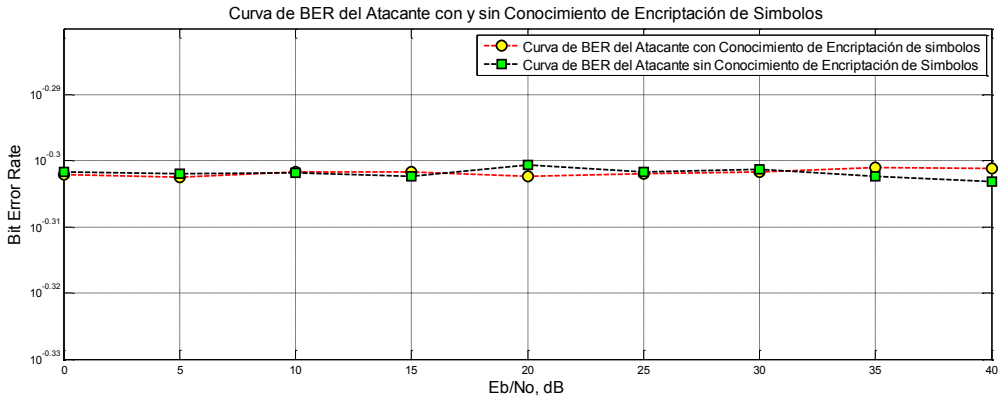

Figura 5.17.: Curva de BER del atacante con conocimiento de encriptación de datos

6. Conclusiones y trabajos futuros

De acuerdo a lo presentado en los capítulos anteriores se desprenden las siguientes conclusiones:

1. Los estimadores presentados alcanzan un error cuadrático aceptable sobre un sistema OFDM. El estimador MMSE al tener un conocimiento a priori de la varianza del ruido y la covarianza del canal logra obtener un menor error de estimación en comparación que el LSE, esto lo hace beneficioso dado que es necesario tener un conocimiento casi perfecto del canal de propagación en el transmisor ya que el canal es la clave que permite proveer seguridad en la comunicación. Sin embargo esto trae consigo una mayor complejidad en comparación al estimador LSE.
2. El uso de la Descomposición en Valores Singulares del Canal de Propagación único entre el Transmisor y Receptor legítimo permite obtener matrices que encriptan y desencriptan la información que se transmite, lo que permite que el error de un atacante sea constante para diferentes valores de E_b/N_o, asegurando que el atacante no pueda desencriptar la información.
3. Es factible implementar seguridad a nivel de capa física en OFDM usando la SVD del canal de propagación. La seguridad brindada por el mecanismo propuesto es evaluada a través de los valores de BER del receptor legítimo y del atacante.
4. En los resultados que se han obtenido se muestra que los valores de BER del atacante son altos en comparación con los valores de BER del receptor legítimo, esto debido a que el atacante al no tener conocimiento del canal del receptor legítimo, trata de desencriptar la información a través de las matrices obtenidas por la SVD de su propio canal H_{ka}.
5. El mecanismo de seguridad basado en la rotación de constelación y el método propuesto presentan curvas de BER para el atacante casi constante para diferentes valores de E_b/N_o. En tanto, para el caso del receptor legitimo el mecanismo de rotación presenta una ganancia de codificación de 10 dB aprox., esto se da debido a que las condiciones de simulación presentadas por este método asume conocimiento de canal y sincronización perfecta en transmisión/recepción.

Como posibles trabajos futuros se consideran los siguientes puntos.

1. En las simulaciones realizadas se ha usado dos nodos en presencia de un espía, por lo que se propone extender a múltiples nodos en presencia de múltiples es-

pías de tal forma que se pueda evaluar la influencia de estos sobre los resultados obtenidos.

2. Realizar simulaciones de capa física para diferentes estándares de comunicación inalámbrica que utiliza OFDM como LTE, Wi-MAX, IEEE 802.11n entre otros y analizar los resultados obtenidos y compararlos con trabajos previos.

3. Analizar los tiempos referidos a los procesos de estimación de canal y la aplicación de la SVD en el nodo transmisor.

4. En el apartado 2.5.3 se desarrollaron algoritmos de estimación de canal que no son adaptativos y se realizó la simulación con estos algoritmos de estimación utilizando un canal con desvanecimiento plano (Retardo esparcido $\tau_n <$ Período de símbolo). Sin embargo, cuando se trata de canales selectivos en frecuencia (Retardo esparcido $\tau_n >$ Período de símbolo), resulta interesante la posibilidad de poder adaptar las características espectrales de la señal transmitida a la forma que el canal tiene en cada momento, y ello se consigue con algoritmos de estimación de canal adaptativos como el LMS (Least Mean Squares) y RLS (Recursive Least Square).

Reconocimientos

El presente trabajo de tesis me gustaría agradecer principalmente a Dios por haberme dado la vida y por seguir acompañándome en este largo camino, brindádome sabiduría, conocimiento y paciencia para continuar luchando por cada uno de los sueños que más anhelo.

Deseo expresar mi profundo agradecimiento al Dr. Alex Cartagena por su confianza, su paciencia y su valiosa ayuda en la elaboración de este trabajo ya que sin sus innumerables sugerencias no hubiera sido posible.

De igual manera a mis grandes amigos Jaime, Arthur, y Raúl por su tiempo para escucharme, su tolerancia para entenderme y sus innumerables enseñanzas tanto a nivel personal como profesional. Así también a mis compañeros de la Universidad, por los excelentes momentos y horas de trabajo que he compartido a lo largo de estos años.

A mis hermanos Yensi, Juliana y Vania mi eterno agradecimiento por su apoyo incondicional, motivación e innumerables consejos en momentos difíciles.

Finalmente, no existen palabras para expresar mi gratitud a Juana y Francisco, mis padres, por darme una vida feliz, creer en mí, enseñarme el valor de la perseverancia, de la educación, del trabajo, del sacrificio... y sobre todo del amor.

A. Anexo

Este apartado desarrolla y demuestra el proceso matemático en el cual un receptor legítimo puede decodificar los datos enviados. Esta afirmación nos ubica en el siguiente caso. Cuando un transmisor encripta los símbolos OFDM con la matriz V_k , el atacante intentará desencriptar los símbolos, pero dado que éste con otra matriz desencriptadora generada de su descomposición matricial no podrá realizar tal proceso.

Mediante el uso de la descomposición SVD, descomponemos el canal de comunicación entre el transmisor y el receptor legítimo en tres matrices representadas de la siguiente forma:

$$H_k = U_k \Delta_k V_k^T \tag{A.1}$$

donde U_k y $V_k$son matrices cuadradas de dimensiones $k\,x\,k$ que contienen los vectores singulares: izquierdo y derecho del canal $H_k$respectivamente. La matriz diagonal cuadrada Δ_k de dimensiones $k\,x\,k$ contiene los valores singulares o eigenvalores. Cada símbolo generado por medio de la modulación OFDM es representado como un vector de $k - elementos$ de la siguiente forma:

$$\hat{x}_k = \left[\hat{x^1}\ \hat{x^2}\ \ldots\ \hat{x^k}\right] \tag{A.2}$$

A continuación se utiliza la matriz V_k,como matriz encriptadora, la cual multiplica a cada símbolo transmitido, con lo que cada símbolo transmitido es:

$$x_k = V_k.\hat{x}_k \tag{A.3}$$

Por lo tanto, los símbolos recibidos al pasar por el canal matricial H_k y al ser sumados por una componente de Ruido AWGN, z_k, serán representados de la siguiente forma:

$$y_k = H_k V_k \hat{x}_k + z_k \tag{A.4}$$

Una vez recibido cada símbolo, se procede a realizar el proceso de desencriptación, ello se logra mutiplicando el símbolo recibido por la matriz W_k, la cual utiliza la matriz unitaria U_k y la matriz diagonal Δ_k.

$$W_k = \Delta_k^{-1} U_k^T \tag{A.5}$$

Para estimar el símbolo recibido se establece la siguiente ecuación:

$$\hat{x_k^e} = W_k y_k \tag{A.6}$$

$$\hat{x_k^e} = W_k \left(H_k V_k \hat{x}_k + z_k\right) \tag{A.7}$$

$$\hat{x_k^e} = W_k \left(U_k \Delta_k \left(V_k^T . V_k\right) \hat{x}_k + z_k\right) \tag{A.8}$$

dado que: $V_k^T . V_k = I$ se tiene:

$$\hat{x_k^e} = W \left(U_k \Delta_k I_k \hat{x}_k + z_k\right) \tag{A.9}$$

$$\hat{x_k^e} = \Delta_k U_k^T \left(U_k \Delta_k \hat{x}_k + z_k\right) \tag{A.10}$$

del mismo modo $U_k^T . U_k = I$, ahora se tiene:

$$\hat{x_k^e} = \Delta_k^{-1} \Delta_k \hat{x}_k + \Delta_k^{-1} U_k^T z_k \tag{A.11}$$

$$\hat{x_k^e} = I_k \hat{x}_k + \Delta_k^{-1} U_k^T z_k \tag{A.12}$$

$$\hat{x_k^e} = \hat{x}_k + \Delta_k^{-1} U_k^T z_k \tag{A.13}$$

Finalmente la señal recibida $\hat{x_k^e}$ en el receptor será:

$$\hat{x_k^e} = \hat{x}_k + \Delta_k^{-1} U_k^T z_k \tag{A.14}$$

Bibliografía

[Agu01] M. Aguayo. Modulación Multiportadora Adaptativa para Canales selectivos en Frecuencia con desvanecimientos. Master's thesis, Universidad de Málaga, 2001.

[Art07] A. Artés. *Comunicaciones Digitales*. Pearson Educacion S.A, 2007.

[Bat09] O. Batalla. Seguridad en 802.11: Estudio y Desarrollo de un Sistema de Gestión para EAP-TLS. Master's thesis, Universidad Politécnica de Catalunya, 2009.

[CM09] J. Cano and P. Manzoni. Redes Inalámbricas Ad Hoc: Una arquitectura para dar soporte a las Aplicaciones Ubicuas, 2009.

[Cor09] M. Cordero. Técnicas de estimación de Canal en la Capa Física Wireless MAN-OFDM de la norma IEEE 802.16e. Master's thesis, Universidad de Sevilla, 2009.

[CWH+11] S. Chang, S. Wu, S. Huang, H. Hwa, and Y. Chen. Physical Layer Security in Wireless Networks: A Tutorial. *Wireless Communications*, 18(7): 66–74, 2011.

[Dez07] E. Deza. Estudio de Aplicaciones de Redes de Comunicaciones Inalámbricas Ad-Hoc para Sistemas a bordo de Automóviles. Master's thesis, Universidad Politécnica de Catalunya, 2007.

[Esp11] R. Espinoza. Uso de un FPGA para la Implementación de la Sección de Banda Base de la Capa física de un Transmisor basado en el estándar IEEE 802.11n en modo Greenfield. Master's thesis, Escuela Politécnica Nacional, Quito, 2011.

[FS02] P. Flikkema and C. Sperandio. Wireless Physical-Layer security via Transmit Precoding over Dispersive Channels: Optimum Linear Eavesdropping. *Military Communications Conference*, 2(7): 1113–1117, 2002.

[GA04] J. Geier and D. Akin. *Certified Wireless Analysis Professional Official Study Guide (Exam PW0-205)*. McGraw-Hill, 2004.

[Gar] J. Garcia. Algebra lineal numerica con MATLAB.

[Gar10] C. Garcia. Impacto de la Seguridad en Redes Inalámbricas de Sensores IEEE 802.15.4. Master's thesis, Universidad Complutense de Madrid, 2010.

[GK11] S. Gollakota and D. Katabi. Physical Layer Wireless Security made Fast and Channel Independent. *International Conference on Computer Communications*, 1(7): 1125–1133, 2011.

[Goe07] S. Goel. Guaranteeing Secrecy in Wireless Networks using Artificial Noise. Master's thesis, Carnegie Mellon University, 2007.

[Her] R. Hernando. Seguridad en Redes inalámbricas.

[IEE03] IEEE. Wireless LAN Medium Access Control and Physical Layer Specifications. IEEE 802.11 Standard: http://ieeexplore.ieee.org/servlet/opac?punumber=9543 1, 2003.

[ITU91] ITU. Security Architecture for Open Systems Interconnection. Recommendation X.800. https://www.itu.int/rec/t-rec-x.800-199103-i/en, 1991.

[JST10a] S. Jarot, M. Siddigi, and M. Tahir. Wireless Physical Layer Security using Chanel State Information. *International Conference on Computer and communication Engineering*, 1(7): 1–5, 2010.

[JST10b] S. Jarot, M. Siddigi, and M. Tahir. Wireless Physical Layer Security using Encryption and Channel Pre-Compensation. *Computer Applications and Industrial Electronics*, 1(7): 304–309, 2010.

[LDRV07] W. López, Y. Da Rocha, and C. Vargas. Sistemas de Comunicación inalámbrica MIMO - OFDM, 2007.

[Man08] A. Manjón. Estudio y Simulación de la Tecnologia WiFi de Acceso Inalámbrico. Master's thesis, Universidad Politécnica de Catalunya, 2008.

[Mat] Matworks. The Language of Technical Computing.

[Mat13] M. Mathuranathan. *Simulation of Digital Communication System using MATLAB*. Mathuranathan Viswanathan at Gaussianwaves, 2013.

[Mia06] G. Miao. *Signal Processing for Digital Communications*. Artech House, 2006.

[Mic14] K. Mickelberg. 2014/ USomputer State of Ciber Crimen., 2014.

[MMA07] A. Martinez, V. Morales, and G. Aguilar. Sistema Detección de Intrusos para una Red Inalámbrica de una PyME. Master's thesis, Instituto Politécnico Nacional, 2007.

[Paz11] A. Pazmiño. Aplicaciones de Hacking Etico para la determinación de Vulnerabilidades de Acceso a Redes inalámbricas WiFi. Master's thesis, Escuela Superior Politécnica de Chimborazo, 2011.

[Pol11] A. Polbach. Estimación ciega de Canal en Sistemas OFDM. Master's thesis, Universidad Politécnica de Catalunya, 2011.

[Pov00] J. Poveda. Espectro ensanchado. *Ingeniería*, 5(1): 71–78, 2000.

[Pra10] N. Prasad. State of the Art of the Wireless Security in OFDM(A)-based Systems. *Mobile WiMAX Symposium*, 2(7): 107–110, 2010.

[QP08] G. Quintanar and M. Pacheco. Seguridad en la Red inalámbrica de esime azcapotzalco. Master's thesis, Instituto Politécnico Nacional, 2008.

[RL05] P. Ratazzi and X. Li. MIMO Transmissions with Information-Theoretic Secrecy for Secret-Key Agreement in Wireless Network. *Military Communications*, 1(7): 1353–1359, 2005.

[Sán00] J. Sánchez. CDMA: Comunicaciones de Espectro Ensanchado. *Buran*, 16(7): 25–32, 2000.

[Str04] L. Strand. Adaptive Distributed Firewall using Intrusion Detection. Master's thesis, University of Oslo, 2004.

[Val10] C. Valverde. Implementacion de un sistema OFDM en un dispositivo SFF-SDR. Master's thesis, Universidad Carlos III, 2010.

[Ver08] J. Vergara. Simulación de un esquema de Modulación/Demodulación OFDM utilizando un Modelo de Canal Multitrayectoria. Master's thesis, Escuela Superior Politécnica del Litoral, 2008.

[VFA08] T. Vakili, A. Falahati, and D. Abbasi. Combination of Turbo Coding and Cryptography in Non-Geo Satellite Communication Systems. *International Symposium Telecommunications*, 1(7): 666–667, 2008.

[Vie] J. Vieitez. Descomposicion LU de Matrices.

[VL11] J. Villón and A. Loaiza. Usando Single Value Decomposition, proponer una señal que permita idealmente cancelar casi cualquier tipo de Interferencia en un Canal alámbrico. Master's thesis, Escuela Superior Politécnica del Litoral, 2011.

[VM] M. Villegas and M. Marmolejo. Tópicos en Algebra Lineal.

[YWG+15] N. Yang, L. Wang, G. Geraci, M. Elkashlan, and M. Yuan, J. Di Renzo. Safeguarding 5G Wireless Communication Networks using Physical Layer Security. *IEEE Communications Magazine*, 2015.

[ZAG06] A. Zaim, A. Aydin, and Z. Gurkas. Security Mechanisms and their Performance Impacts on Wireless Local Area Networks. *International Symposium on Computer Networks*, 2: 1–5, 2006.

Nomenclatura

AES	Advanced Encryption Standard
AWGN	Additive White Gaussian Noise
BER	Bit Error Rate
BER	Bit Error Rate
BPSK	Binary Phase Shift Key
CCA	Clear Channel Assessment
CCMP	Counter Mode with CBC-MAC Protocol
CSMA/CA	Carrier Sense Multiple Access/ Collision Avoidance
DFT	Discrete Fourier Transform
FFT	Fast Fourier Transform
FIR	Finite Impulse Response
ICI	Intercarrier Interference
IDFT	Inverse Discrete Fourier Transform
ISI	Inter Symbol Interference
LLC	Logical Link Control
LSE	Least Squares Error
MAC	Medium Access Control
MIMO	Multiple Input Multiple Output
ML	Maximum Likelihood
MMPDU	MAC Management Protocol Data Unit
MMSE	Minimum Mean Square Error

MSDU	MAC Service Data Unit
OFDM	Orthogonal Frecuency Division Multiplexing
OFDM	Othogonal Frecuency Division Multiplexing
PLCP	Physical Layer Convergence Protocol
PMD	Physical Medium Dependent
PSAM	Pilot Symbol Assisted Modulation
QoS	Quality of Service
RADIUS	Remote Authentication Dial In User Service
RC4	River Cipher 4
SSH	Secure Shell
SSL	Secure Socket Layers
SVD	Single Value Descomposition
TKIP	Temporary Key Integrity Protocol
WLAN	Wireless Local Area Network
WMAN	Wireless Metropolitan Area Network
WPAN	Wireless Personal Area Network